(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 September 2004 (02.09.2004)

PCT

(10) International Publication Number
WO 2004/075049 A1

(51) International Patent Classification[7]: G06F 9/445, 12/14

(21) International Application Number: PCT/AU2004/000210

(22) International Filing Date: 20 February 2004 (20.02.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2003900764 20 February 2003 (20.02.2003) AU

(71) Applicant *(for all designated States except US)*: **SECURE SYSTEMS LIMITED** [AU/AU]; Level 1, 80 Hasler Road, Osborne Park, Western Australia 6017 (AU).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KABZINSKI, Richard** [AU/AU]; 5 Balladonia Drive, Ellenbrook, Western Australia 6069 (AU). **HEARN, Michael, Alfred** [AU/AU]; 1 Urawa Road, Duncraig, Western Australia 6023 (AU). **POWERS, Russell, E** [AU/AU]; Level 1, 80 Hasler Road, Osborne Park, Western Australia 6017 (AU).

(74) Agent: **WRAY & ASSOCIATES**; Level 4, The Quadrant, 1 William Street, Perth, Western Australia 6000 (AU).

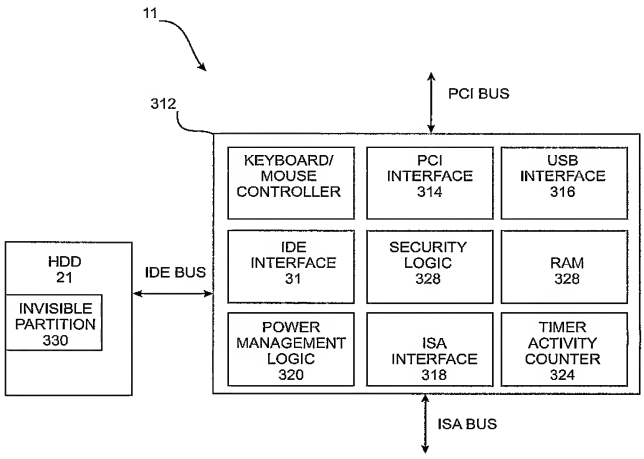
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: BUS BRIDGE SECURITY SYSTEM AND METHOD FOR COMPUTERS



(57) Abstract: A computer security system comprising security logic that is independent of the host CPU (13) for controlling access between the host CPU (13) and the storage device (21). A program memory (41) that is independent of the computer memory unalterably stores and provides computer programs for operating the processor (37) in a manner so as to control access to the storage device (21). The security logic comprises logic in bus bridge circuitry . The bus bridge circuitry can be embodied in the south bridge circuit (326) of a computer system (11) or alternatively in a SOC circuit (351) of a HDD. All data access by the host CPU (13) to the data storage device (21) is blocked before initialisation of the security system and is intercepted immediately after the initialisation under the control of the security logic. The security logic effects independent control of the host CPU (13) and configuration of the computer (11) to prevent unauthorised access to the storage device (21) during the interception phase. All users of the computer (11) are authenticated with a prescribed profile of access to the storage device (21) and data access to the storage device remains blocked until a user of the computer (11) is correctly authenticated.

WO 2004/075049 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

"Bus Bridge Security System and Method for Computers"

Field of the Invention

This invention relates to a security system for securing data and information stores in computer systems and a method of securing the same. More specifically, the invention relates to a security system for a computer having bus bridge circuitry.

In the context of this specification, a computer system is defined to include a computer having a central processing unit (CPU) and a storage device, which may be a hard disk, CD R/W or other read/writeable data storage media or any combination of the same, and a network incorporating one or more such computers, as in a client server system.

In conventional computer systems the CPU typically requires one or more support chips to handle bus interfacing and arbitration, and caching and buffering of data from memory. These functions are normally managed by chipsets that perform a "bridging" function. In particular, bridge circuitry may provide an interface between two independent buses.

Throughout the specification, unless the context requires otherwise, the word "comprise" or variations such as "comprises" or "comprising", will be understood to imply the inclusion of a stated integer or group of integers but not the exclusion of any other integer or group of integers.

Background Art

The proceeding discussion of the background art is intended to facilitate an understanding of the present invention only. It should be appreciated that the discussion is not an acknowledgement or admission that any of the material referred to was part of the common general knowledge in Australia as at the priority date of the application.

In these days of widespread computer usage, data stored on a computer system is becoming increasingly accessible to a variety of users. This may occur directly in real time via local and/or remote use of a computer system by different users or indirectly via the loading and running of computer programs at predetermined times automatically or manually by a user of the computer system. With the advent of computer networks allowing remote access to computer systems via local area networks and wide area networks such as the Internet, and the ready transfer of computer programs and data between computer systems, either manually via floppy disks and CD ROMs or automatically via computer networks, the security and integrity of data and information stored on the read/write stores of computers is becoming increasingly of paramount importance.

It is now common place for computer systems to incorporate "anti-virus" software in order to protect the data and information stored on the storage device thereof from hostile computer programs, and user authentication procedures allowing predetermined levels of access to data and information stored on the storage device of the computer system, dependent upon the status of the user.

A problem with most types of anti-virus software and user authentication protocols used today is the very fact that they are embodied in software, which is required to be executed under the control of the operating system of the computer. Hence, a pre-requisite for such anti-virus or user authentication software to function correctly is that the computer system must be able to power-on, boot-up and invoke the operating system "cleanly", without any virus or security defeating processes affecting the computer during this time.

In the case of anti-virus software, most of this software depends upon having some knowledge of the virus or type of virus that it is attempting to secure the system from. Hence, the anti-virus software needs to be constantly updated and entered onto the computer system before a particular virus finds its way to the computer system.

As certain viruses can be extremely hostile and destructive to computer systems, the lag time between the first occurrence of a virus and the production of software

to combat the virus still creates a window within which oftentimes irreparable damage can occur to certain computer systems infected with such a virus. Indeed, the production of viruses and anti-virus software does have a tendency to be self-perpetuating. Thus whilst better solutions may have been proposed in the past to combat viruses and ensuring the security of data and information, the state of the art has remained around adopting a software approach to deal with the problem.

Notwithstanding this, various hardware-based solutions, which are intrinsically more reliable and resilient in preventing virus or unauthorised access to data stored on a computer system, have been proposed in the past. However, these have been awkward to apply, restricted in their adaptability to different and changing formatting standards or have required user interaction of a technical nature well beyond the mere loading of executable programs, in order to make them effective or even operational.

WO 03/003242 by this applicant, which is incorporated herein by reference, discloses a security device to control access to stored data during boot-up, and also in real-time after the operating system has been loaded. The security device in 03/003242 uses its own discrete dedicated circuitry for processing, memory and bus control and interface.

It would be advantageous to provide boot and real-time control of data access without discrete dedicated circuitry.

Disclosure of the Invention

It is an object of the present invention to provide robust protection for data and information stored on a computer system from unauthorised access and/or misuse using the circuitry of the computer system itself.

In accordance with one aspect of the present invention, there is provided a security system for a computer having a host central processing unit (CPU), memory used by the host CPU to load programs in order to operate the computer,

a storage device for storing data to be handled by the computer, and a bridge circuit interposed between a first bus connected to the host CPU and a second bus connected to the storage device, the security system comprising:

processing means independent of the host CPU for controlling access between the host CPU and the storage device; and

program memory means independent of the memory of the computer to unalterably store and provide computer programs for operating the processing means in a prescribed manner to control said access;

wherein the processing means comprises logic in the bridge circuit.

Preferably, the security system includes memory store means independent of the memory means of the computer to store critical data and control elements associated with the basic operation of the computer and access to the storage device. Preferably, the memory store means is connected to or included in the bridge circuit.

Preferably, said critical data and control elements are supplied to and used by the host CPU for verification of the storage device and operating the computer independently of the storage device during the start up sequence of the computer.

Preferably, the security system comprises authentication means to authenticate a user of the computer having a prescribed profile of access to the storage device. Preferably, the authentication means comprises logic in the bridge circuit.

Preferably, the authentication means includes a login verifying means to enable a user of the computer to enter a login identification and password and have that login identification and password verified to authenticate said user being an authorised user of the computer having a prescribed profile of access to the storage device before allowing the start up sequence of the computer to proceed further.

Preferably, said login identification and passwords of authorised users and the prescribed profile of access thereof form part of said critical data and control elements and said login verifying means accesses said critical data and control elements to effect authentication of a user.

Preferably, the prescribed profile of access comprises a prescribed allocation of predetermined levels of access permitted for an authorised user of the computer to prescribed partitions or zones of the storage device.

Preferably, the security system includes intercepting means to block all data access by the host CPU to the data storage device before initialisation of the security system and intercept all said data access immediately after said initialisation under the control of said processing means. Preferably, the intercepting means comprises logic in the bridge circuit.

Preferably, said critical data and control elements include identification data in respect of the storage device for enabling the computer to complete its peripheral check during said start up sequence.

Preferably, said critical data and control elements include a custom boot sector that includes invoking said authentication means for assuming operation of the computer during said start up sequence.

Preferably, the authentication means includes an authentication application program stored in the program memory means, the memory store means or the storage device.

Preferably, the authentication application program includes user editing means to enable an authorised user having a particular prescribed level of access to create and edit authorised users for accessing the storage device.

Preferably, the authentication application program includes access profile editing means to enable said authorised user having a particular prescribed level of access to allocate and edit particular predetermined levels of access to said

prescribed partitions or zones for all authorised users having access to the storage device.

In accordance with another aspect of the present invention, there is provided a method for securing and protecting a storage device for storing data to be handled by a computer from unauthorised access, the computer having a host central processing unit (CPU), memory used by the host CPU to load programs in order to operate the computer and storage device, and a bridge circuit interposed between a first bus connected to the host CPU and a second bus connected to the storage device, the method comprising:-

controlling access between the host CPU and the storage device independently of the host CPU using logic in the bridge circuit; and

unalterably storing computer programs for effecting said controlling access in a location separate from the memory and not addressable by the host CPU.

Preferably, the method includes storing critical data and control elements associated with the basic operation of the computer and access to the storage device in a location separate from the memory and not addressable by the host CPU. Preferably, the method includes storing the critical data and control elements in memory store means connected to the bridge circuit. Preferably, the method includes storing the critical data and control elements in the bridge circuit.

Preferably, the method includes independently supplying the host CPU with said critical data and control elements for verification of the storage device and operating the computer independently of the storage device during the start up sequence of the computer.

Preferably, the method includes authenticating a user of the computer having a prescribed profile of access to the storage device.

Preferably, said authenticating includes enabling a user of the computer to enter a login identification and password and verifying the same to establish whether the user is an authorised user of the computer having a prescribed profile of access to the storage device before allowing the start up sequence of the computer to proceed further.

Preferably, said login identification and passwords of authorised users and the prescribed profile of access thereof form part of said critical data and control elements and the verifying includes comparing the entered login identification and password with the login identification and passwords within said critical data and control elements and authenticating a user if there is match.

Preferably, the prescribed profile of access comprises a prescribed allocation of predetermined levels of access permitted for an authorised user to prescribed partitions or zones of the storage device.

Preferably, the method includes blocking all data access by the host CPU to the data storage device during initialisation of the computer and intercepting all said data access during the start up sequence after said initialisation.

Preferably, said critical data and control elements include identification data in respect of the storage device for enabling the computer to complete its peripheral check during said start up sequence.

Preferably, said critical data and control elements include a custom boot sector for the computer that includes invoking the authenticating step; and the method includes assuming operation of the computer during said start up sequence with the custom boot sector and authenticating the user of the computer at such time.

Preferably, said authenticating includes enabling a particular prescribed level of authorised user to create and edit login identifications and passwords within the critical data and control elements for specifying authorised users having access to the storage device.

Preferably, said authenticating includes enabling said particular prescribed level of authorised user to allocate and edit particular predetermined levels of access to said prescribed partitions or zones for all authorised users having access to the storage device within the critical data and storage elements.

Preferably, user authentication is performed only in the bridge circuit.

In accordance with a further aspect of the present invention, there is provided a security system for a computer having a host central processing unit (CPU), memory used by the host CPU to load programs in order to operate the computer, a storage device for storing data to be handled by the computer, and a bridge circuit interposed between a first bus connected to the host CPU and a second bus connected to the storage device, the security system comprising:

processing means independent of the host CPU for controlling access between the host CPU and the storage device; and

intercepting means to block all data access by the host CPU to the data storage device before initialisation of the security system and intercept all said data access immediately after said initialisation under the control of said processing means;

wherein said processing means effects independent control of the host CPU and configuration of the computer in a manner so as to prevent unauthorised access to the storage device on said intercepting means intercepting said data access immediately after said initialisation; and

wherein the processing means and intercepting means comprise logic in the bridge circuit.

Preferably, the security system includes program memory means independent of the memory of the computer to unalterably store and provide computer programs for operating the processing means in a prescribed manner to control said access. Preferably, the program memory means is connected to or included in the bridge

circuit. Preferably, the prescribed profile of access comprises a prescribed allocation of predetermined levels of access permitted for an authorised user of the computer to prescribed partitions or zones of the storage device.

Preferably, the bridge circuit is adapted to be connected only in line with the data access channel between the host CPU and the storage device, and off the main data and control bus of the host CPU.

In accordance with another aspect of the present invention, there is provided a method for securing and protecting a storage device for storing data to be handled by a computer from unauthorised access, the computer having a host central processing unit (CPU), memory used by the host CPU to load programs in order to operate the computer and storage device, and a bridge circuit interposed between a first bus connected to the host CPU and a second bus connected to the storage device, the method comprising:-

controlling all data access between the host CPU and the storage device independently of the host CPU;

blocking all data access by the host CPU to the storage device during initialisation of the computer; and

intercepting all said data access during the start up sequence after said initialisation to effect independent control of the host CPU and configuration of the computer in a manner so as to prevent unauthorised access to the storage device thereafter;

wherein all data access is controlled, blocked and intercepted by logic in the bridge circuit.

Preferably, the method includes unalterably storing computer programs for effecting said controlling access in a location separate from the memory and not addressable by the host CPU. Preferably, the method includes unalterably storing computer programs for effecting said controlling access in memory store means

connected to the bridge circuit. Preferably, the method includes unalterably storing computer programs for effecting said controlling access in the bridge circuit.

Preferably, said login identification and passwords of authorised users and the prescribed profile of access thereof form part of said critical data and control elements and the verifying includes comparing the entered login identification and password with the login identification and passwords within said critical data and control elements and authenticating a user if there is match.

Preferably, the prescribed profile of access comprises a prescribed allocation of predetermined levels of access permitted for an authorised user to prescribed partitions or zones of the storage device.

Preferably, user authentication is performed only in the bridge circuit.

In accordance with another aspect of the present invention, there is provided a security system for a computer having a host central processing unit (CPU), memory used by the host CPU to load programs in order to operate the computer, a storage device for storing data to be handled by the computer, and a bridge circuit interposed between a first bus connected to the host CPU and a second bus connected to the storage device, the security system comprising:

blocking means for selectively blocking data access between the host CPU and the storage device; and

authentication means to authenticate a user of the computer having a prescribed profile of access to the storage device;

wherein said blocking means maintains said blocking data access until said authentication means completes correct authentication of the user of the computer; and

wherein the blocking means comprises logic in the bridge circuit.

selectively blocking all data access between the host CPU and the storage device using logic in the bridge circuit; and

authenticating a user of the computer having a prescribed profile of access to the storage device;

wherein said blocking of data access is maintained until the user of the computer is correctly authenticated.

Preferably, said selective blocking comprises controlling access between the host CPU and the storage device independently of the host CPU.

Preferably, said selective blocking occurs during initialisation of the computer and includes intercepting all said data access during the start up sequence immediately after said initialisation and before loading of the operating system of the computer to enable independent control of the host CPU and configuration of the computer in a manner so as to prevent unauthorised access to the storage device.

Preferably, the method includes performing a software boot of the computer after correct authentication of the user, and allowing normal loading of the operating system during the start up sequence of the computer thereafter.

Preferably, the method includes controlling blocking access to the storage device after correct authentication of the user in accordance with the prescribed profile of access of the user.

Preferably, the method includes unalterably storing computer programs for effecting said controlling access in a location separate from the memory and not addressable by the host CPU. Preferably, the method includes unalterably storing computer programs for effecting said controlling access in memory store means connected to the bridge circuit. Preferably, the method includes unalterably storing computer programs for effecting said controlling access in the bridge circuit.

Preferably, the security system includes processing means independent of the host CPU for controlling the operation of said blocking means for blocking access between the host CPU and the storage device in response to said authentication means. Preferably, the processing means comprises logic in the bridge circuit.

Preferably, the authentication means comprises logic in the bridge circuit.

Preferably, the blocking means blocks all data access by the host CPU to the data storage device before initialisation of the security system and includes intercepting means to intercept all said data access immediately after said initialisation under the control of said processing means.

Preferably, said processing means effects independent control of the host CPU and configuration of the computer in a manner so as to prevent unauthorised access to the storage device, upon said intercepting means intercepting said data access immediately after said initialisation and before loading of the operating system of the computer.

Preferably, said authentication means enables a software boot of the computer to be effected after correct authentication of the user, and said processing means permits normal loading of the operating system during the start up sequence of the computer following said software boot.

Preferably, said processing means controls said blocking means to effect blocking access to the storage device after correct authentication of the user in accordance with the prescribed profile of access of the user.

Preferably, the security system includes program memory means independent of the memory of the computer to unalterably store and provide computer programs for operating the processing means in a prescribed manner to control said access. Preferably, the program memory means is connected to or included in the bridge circuit.

Preferably, the security system includes memory store means independent of the memory means of the computer to store critical data and control elements associated with the basic operation of the computer and access to the storage device. Preferably, the memory store means is connected to or included in the bridge circuit.

Preferably, said critical data and control elements are supplied to and used by the host CPU for verification of the storage device and operating the computer independently of the storage device during the start up sequence of the computer.

Preferably, the authentication means includes a login verifying means to enable a user of the computer to enter a login identification and password and have that login identification and password verified to authenticate said user being an authorised user of the computer having a prescribed profile of access to the storage device before allowing the start up sequence of the computer to proceed further.

Preferably, said login identification and passwords of authorised users and the prescribed profile of access thereof form part of said critical data and control elements and said login verifying means accesses said critical data and control elements to effect authentication of a user.

Preferably, the prescribed profile of access comprises a prescribed allocation of predetermined levels of access permitted for an authorised user of the computer to prescribed partitions or zones of the storage device.

In accordance with another aspect of the present invention, there is provided a method for securing and protecting a storage device for storing data to be handled by a computer from unauthorised access, the computer having a host central processing unit (CPU), memory used by the host CPU to load programs in order to operate the computer and storage device, and a bridge circuit interposed between a first bus connected to the host CPU and a second bus connected to the storage device, the method comprising:-

Preferably, said authenticating includes enabling a user of the computer to enter a login identification and password and verifying the same to establish whether the user is an authorised user of the computer having a prescribed profile of access to the storage device before allowing the start up sequence of the computer to proceed further.

Preferably, said login identification and passwords of authorised users and the prescribed profile of access thereof form part of said critical data and control elements and the verifying includes comparing the entered login identification and password with the login identification and passwords within said critical data and control elements and authenticating a user if there is match.

Preferably, the prescribed profile of access comprises a prescribed allocation of predetermined levels of access permitted for an authorised user to prescribed partitions or zones of the storage device.

Preferably, user authentication is performed only in the bridge circuit.

A bus bridge circuit for bridging data access between different buses or interfaces of a computer having a host CPU or a computer storage device, and for protecting unauthorised accesses of said computer storage device by said computer, the circuit comprising:

processing means for controlling operation of the circuit;

memory for loading application programs therein to be run by said processing means;

first interface means for interfacing the circuit with a first bus or device structure to communicate with the host CPU of the computer;

second interface means for interfacing the circuit with a second bus or device structure to communicate with the computer storage device; and

security logic means for controlling data access between said first interface means and said second interface means, in accordance with a prescribed application program run by said processing means, to prevent unauthorised data access to said computer storage device.

Preferably, said prescribed application program is initially stored remotely of said bus bridge circuit in a hidden location within the storage device, and said security logic means is configured to load said application program into said memory means on setting of said bus bridge circuit.

Preferably, said logic security means is configured to provide blocking means to block communications between said first interface means and said second interface means by default, and selectively allow controlled communications between said first interface means and said second interface means in accordance with said application software, after loading and running thereof by said processing means.

Preferably, said security logic means forms intercepting means to block all data access by the host CPU to the data storage device before initialisation of the bus bridge circuit and intercept all said data access immediately after said initialisation under the control of said processing means.

Preferably, said prescribed software application provides for authentication means to authenticate a user of the computer having a prescribed profile of access to the storage device, and said blocking means maintains said blocking data access until said authentication means completes correct authentication of the user of the computer.

Brief Description of the Drawings

The invention will be better understood in the light of the following description of one specific embodiment thereof. The description is made with reference to the following drawings, wherein:-

Figure 1 is a schematic box diagram of a typical computer system showing the physical location of the security device disclosed in WO 03/003242 relative to the host CPU, main bus, interface logic and various peripheral devices;

Figure 2 is a schematic box diagram of the security device disclosed in WO 03/003242 showing its general functional make-up;

Figure 3 is a schematic box diagram of a typical computer system having bus bridge architecture comprising multiple buses and bus bridge circuits;

Figure 4 is a schematic box diagram of a bus bridge circuit according to a first embodiment of the present invention within a computer system of the type shown in Figure 3;

Figure 5 is a flow chart showing the start up sequence of a normal computer that is not equipped with the security system of the present invention;

Figures 6A and 6B are flow charts showing the start up sequence of a computer system equipped with the security system of the present invention;

Figure 7 is a flow chart showing the various states of operation of the security system of the present invention from power on;

Figure 8 is a flow chart showing the various processes performed by the authentication application program;

Figure 9A shows the graphical specification format of the general login graphical user interface (GUI) screen;

Figure 9B shows the graphical specification format of the normal user type login GUI screen;

Figure 9C shows the graphical specification format of the administrator type login GUI screen;

Figure 9D shows the graphical specification format of the administrator's user edit GUI screen;

Figure 9E shows the specification format for the administrator's access edit GUI screen; and

Figure 10 is a schematic box diagram of a bus bridge circuit according to a second embodiment of the invention.

Best Mode(s) for Carrying Out the Invention

The best mode of the invention is directed towards a personal computer (PC) system incorporating a security system for protecting a storage media of the computer system, which in the case of a PC may be one or more storage devices generally in the form of a hard disk drive (HDD). The best mode of the security system of the present invention may be embodied in one of two ways, which will be separately described hereinafter. However, before describing the embodiments in detail, the general function of the security system is best explained by first considering the security device disclosed in WO 03/003242.

As shown in Figure 1 of the drawings, the computer system 11 generally comprises a central processing unit (CPU) 13 and a plurality of peripheral devices, which are connected via a main CPU address and data bus 15. The peripheral devices include a monitor 17, a keyboard 19 and one or more storage devices 21. In the current state of the art, typically the storage devices 21 communicate according to the ATA (AT attachment) standard and thus require an ATA channel to be provided between them and the remainder of the computer system 11.

These peripheral devices are connected to the main CPU bus 15 via appropriate interface logic 23, 27 and 31, each comprising decode logic and device I/O (input/output). The interface logic is characterised to allow communication between the CPU 13 and the particular peripheral device.

In the case of the monitor 17, the interface logic 23 therefor is integrated with a video adapter and is connected via a standard video cable 25 to the monitor; in the case of the keyboard 19, the interface logic 27 therefor is integrated with a keyboard port and is connected via an appropriate keyboard cable 29 to the keyboard; and in the case of the storage device(s) 21, the interface logic 31 therefor is integrated with an ATA adapter and is connected via an ATA cable 33 to the storage device(s) to provide the ATA channel.

The security device 35 of WO 03/003242 shown in Figure 1 is physically interposed inline with the ATA cable 33 between the ATA adapter provided on the device interface logic 31 and the storage devices 21. The ATA standard supports most types of storage device, including hard disk drives, CD-ROMS (which actually adopts the ATA/ATAPI enhancement to the ATA standard), flash memory, floppy drives, zip drives and tape drives.

Under the ATA standard, two discrete storage devices may be controlled via the single interface logic 31 and ATA cable 33. Hence reference will be made hereinafter to "storage media", which will comprise either one or two storage devices, and will be used interchangeably with "storage device".

In the case of PC's, the main type of storage device is the HDD. Most HDD's conform to the IDE (Integrated Drive Electronics) hard drive standard or the EIDE (Enhanced IDE) hard drive standard, whereby the controller for the disk drive is located on the HDD itself as opposed to being directly connected to the motherboard of the PC.

Although not shown in the drawings, other embodiments of the computer system 11 may involve storage devices connected to the main computer system via a SCSI (Small Computer Systems Interface) standard, which has its own corresponding interface logic. Accordingly, in the case of storage devices connected to the PC in this manner, the security device 35 of WO 03/003242 would similarly be interposed between the SCSI drive device and the interface logic thereof.

As shown in Figure 2 of the drawings, the security device 35 disclosed in WO 03/003242 generally comprises a CPU 37, RAM (random access memory) 39, flash ROM (read only memory) 41 and bus control and interface logic 43, which in the present embodiment is adapted to the ATA standard for the purposes of protecting the ATA storage device 21. The bus control and interface logic is typically embodied in FPGA (Field Programmable Gate Array) and/or ASIC (Application Specific Integrated Circuit) devices that are connected so as to intercept and permit control of all communications between the host CPU 13 and the disk storage devices 21 under the control of the security device CPU 37.

The security device 35 also includes a secure media interface 45 that allows a separate secure storage media 47 to be connected to the security device via a custom interface 49.

The security device CPU 37 operates according to a prescribed application program stored in the flash ROM 41 and which is loaded into the RAM 39 on start up and becomes the operating system for the security device. The CPU 37 communicates with the bus control and interface logic 43, which is interposed in line with the ATA cable 33 to intercept communications between the host CPU 13 and the storage media 21. The secure media interface 45 is interposed between the bus control and interface logic 43 and the custom interface 49 to facilitate communications between the host CPU 13 and the secure storage media 47 under the control of the CPU 37. This aspect of the operation of the security device disclosed in WO 03/003242 is the subject of a separate invention and will not be further described herein.

Now describing the first embodiment of the security system according to the present invention reference will be made to Figures 3 to 9. Figure 3 shows a computer system 11 having an alternative but generally equivalent architecture to that shown in Figure 1. The architecture in Figure 3 comprises a plurality of buses including a CPU bus 15, PCI bus 306 and multiple peripheral buses. The peripheral buses include ISA bus 302 and IDE bus (or ATA cable) 33.The CPU bus 15 connects host CPU 13 to CPU/PCI bridge circuit or north bridge 304. North bridge 304 is an ASIC that provides bridging between the CPU bus 15 and

PCI bus 306. North bridge 304 also integrates system functions such as controlling communication between host CPU 13, system memory 308 and AGP (Accelerated Graphics Port) 310.

Similar to north bridge 304, south bridge 312 is an ASIC that provides bridging between PCI bus 306 and ISA bus 302 and IDE bus 33. South bridge 312 also integrates miscellaneous system functions such as counters and activity timers, power management, and various interfaces or controllers to handle communication between devices on the PCI bus 306, ISA bus 302 and IDE bus 33. Connected to IDE bus 33 is HDD storage device 21. Other storage media can be similarly connected to south bridge 312 via peripheral buses.

Figure 4 is a generalised block diagram showing an embodiment of the security system 332 according to the present invention. South bridge 312 includes logic for its conventional bus bridging and system functions including PCI interface 314, IDE interface 31, USB (Universal Serial Bus) interface 316, ISA interface 318, power management logic 320, keyboard/mouse controller 322 and timer logic 324. South bridge 312 may also include logic for other miscellaneous system functions.

South bridge 312 also includes security logic 326 and RAM 328. Security logic 326 is functionally equivalent to CPU 37 and bus control and interface logic 43 of the security device 35 of WO 03/003242 shown in Figure 1. As described below in more detail, security logic 326 can selectively secure accesses between host CPU 13 and protected HDD 21.

Similar to security device 35 of WO 03/003242, security logic 326 operates according to a prescribed application program which is loaded into RAM 328 on start up and becomes the operating system for security logic 326. The prescribed application program is stored in a partition 330 on the protected HDD 21 itself which is invisible to a user and can only be accessed by a designated administrator. The secure invisible HDD partition 330 is described in more detail below. Alternatively, the application program may be stored in south bridge 312 itself or in a separate secure memory (not shown) connected to south bridge 312.

The functionality of the application program stored in invisible HDD partition 330and the operation of the security system 332 will now be described with reference to the remaining drawings.

The application program stored in invisible HDD partition for the security logic in south bridge 312 is generally designed to intercept and control the computer system's boot process and provide authentication by means of a login ID and password before access to the protected storage media is permitted. Accordingly, the location of the security logic 326 in south bridge 312 between the host CPU 13 and the storage media 21 is particularly designed so that the security logic 326 is able to selectively filter all requests for information and data flowing to and from the protected storage media 21. The security logic 326 forwards these requests to the storage media 21 as appropriate, based on predetermined user profiles that are set up by a user having an administrator profile, which profiles are stored within invisible HDD partition 330. These profiles are based on access to different partitions and/or files within the protected storage media 21. Thus the designated administrator can set up data protection on a partition-by-partition and/or file-by-file basis in a manner that will be described in more detail later. Similar to the application program, the user profiles may alternatively be stored in south bridge 312 itself or in a separate secure memory connected to south bridge 312. In order to fully understand the operation of the security system 332 of the present invention, an appreciation is required of the normal boot process followed by a standard computer system. This boot process will now be described with reference to Figure 5 of the drawings.

As shown in Figure 5, the normal start up sequence followed by a PC commences as indicated at step 51 with power on shown at 53. This is also known as a "cold" boot, whereby all left over data from the host CPU's internal memory registers and RAM is cleared and the program counter of the CPU is set with the starting address to commence the boot process. This address is the beginning of a boot program stored permanently in the ROM BIOS (Basic Input Output System).

The next step 55 involves the CPU using the address to find and invoke the ROM BIOS boot program. The ROM BIOS program goes through an initialisation phase

that includes setting up hardware and software interrupt vectors and invoking a series of system checks known as power-on self-tests (POSTs) as represented by step 57.

The POST process involves a series of tests to ensure that the RAM of the PC is functioning properly. It then conducts another series of tests, which instruct the host CPU to check that the various peripheral devices, such as the video card and monitor 17, keyboard 19 and storage media 21, are present and functioning properly.

On completing the POST, the BIOS then looks for addresses of BIOS extensions at step 59 that are held in the ROMs of peripheral devices to see if any of them have an extended BIOS to run.

The first of these BIOS extensions is associated with the video card. This BIOS extension initialises the video card to operate the monitor as shown at step 61.

Upon completing initialisation of the video card, the BIOS then proceeds at step 63 to run other BIOS extensions for those peripheral devices that have them.

The BIOS then proceeds to display the start up screen at step 65, before proceeding with conducting further tests on the system at step 67, including the memory test at step 67, which is displayed on the screen.

The BIOS then performs a "system inventory" or equipment check to determine what type of peripheral hardware is connected to the system at step 69. With respect to HDD storage media, the BIOS program causes the host CPU to interrogate the HDD requesting details such as the drive standard (ATA or SCSI), which level of standard (eg whether it is the old standard ATA 1-3 or the new standard ATA 6) the number of cylinders/heads/sectors, and whether it is capable of running in other modes. This stage of interrogation of the HDD is known as "drive ID".

The BIOS then proceeds to configure "logical" devices, such as Plug and Play devices, at step 71 and displays a message on the screen for each one it finds.

The summary screen is then displayed at step 73 indicating the configuration of the computer system. The BIOS then checks for the specified boot sequence at step 75, where the order of priority of storage media to be checked for the location of a valid boot sector, from which the operating system of the computer may be loaded, is specified. The normal order is to check the floppy disk drive (A:), then the hard disk (C:) or vice versa, or the CD ROM drive.

Having identified the order of priority, the BIOS causes the CPU at step 77 to look for boot information in each drive in sequence until a valid boot sector is located.

The BIOS undertakes this process by invoking the software interrupt vector "int 19 at step 79, which stores the address of the particular peripheral device in a software interrupt vector table that is set up during the initialisation phase of the BIOS.

For example, if the target boot drive is the HDD, the CPU looks for a master boot record or boot sector at cylinder 0, head 0, sector 1 (the first sector on the disk), at the address of the device specified in the table: if it is searching a floppy disk, it obtains the address of the floppy disk drive from the table and looks for a volume boot sector at the same location on the floppy disk.

A valid boot sector is determined by the CPU checking the signature of the "ID byte", which normally comprises the first two bytes of the boot sector. If the signature signifies that a boot sector is present, the CPU then proceeds with loading the boot sector at step 81 into RAM and executes or runs the boot loader at step 83 for loading the various operating system files.

In the case of the DOS operating system, the hidden files MS DOS.SYS, IO.SYS and COMMAND.COM are loaded and executed and then the files CONFIG.SYS and AUTOEXEC.BAT are loaded and run to complete configuration of the

computer system and allowing appropriate application programs to be initiated for subsequent operation of the computer system.

In the case of the security system 332, the security logic 326in south bridge 312 is programmed to block out all access of the host CPU 13 to the protected storage media 21 by intercepting the boot process at an early stage during operation of the BIOS. In addition, the security logic 326 in south bridge 312 provides for a custom boot sector to be loaded into the RAM 308 of the host CPU 13, which then executes an authentication application program requiring correct user authentication before allowing the computer system to proceed with its normal boot sector operation and operating system loading. Since the latter operations require access to the protected storage media 21, this methodology ensures that such access is undertaken only after the supervisory control of the security logic 326 in south bridge 312 has been established on a user-by-user basis.

This manner of operation of the security logic 326 in south bridge 312 is best explained in conjunction with Figures 6A, 6B and 7 of the drawings, which outline the operation of the computer system start up sequence with the security system 332 of the present invention installed in the manner previously described.

In this arrangement, the cold boot process of the computer system 332 commences with the start and power on steps 51 and 53, as in the case of the normal computer start up sequence. At power on, the operating system program stored in invisible HDD partition immediately invokes the security logic in south bridge 312 at step 103 to control and intercept all communications from the host CPU 13 to the storage media along the ATA channel, so that no communications are allowed between the host and the protected storage media 21 along the ATA cable 33 at all during this time. Prior to this time the IDE interface logic 31 is not configured and so no access to the storage media is available prior to or during the initialisation phase of the security system along the ATA cable, in any event.

The security logic 326then places a drive busy signal on the ATA channel to inform the host CPU 13 of the status of the storage media 21 and proceeds with requesting the "drive ID" from the storage media, as shown at step 104.

The operations of the security logic 326 in south bridge 312 during this time occur quite independently of the BIOS, whereby the BIOS proceeds with performing steps 55 through to 69, in accordance with its normal operation, until the "drive ID" check is performed by it at step 69.

During steps 55 to 69, the security logic 326in south bridge 312 continues to block of all data communications from the host CPU 13, or any other external device, with the storage media 21. During this "drive busy" phase, the security logic 326is in a state waiting for the "drive ID" information from the storage device. Once the security logic 326receives the "drive ID" information from the storage media 21, the security logic326 stores this in its RAM 328and asserts a "drive ready" signal on the ATA channel to indicate to the host CPU 13 that the storage media 21 is ready to provide the "drive ID".

If the host CPU 13 has already reached the "drive ID" stage 69 and has been polling the IDE interface logic 31 during the "drive busy" phase for less than the requisite time period, or more normally when the BIOS finally reaches the "drive ID" stage at step 69 after the security logic 326 has signalled the "drive ready" phase on the ATA channel, the host CPU 13 issues a request to the driver interface logic 31 of the "drive ID".

Once this request is made at step 69, the security logic 326 in south bridge 312 intercepts the request at 105, continuing to block access to the storage media 21, and provides the host CPU 13 with the "drive ID" of the HDD(s) at step 106.

The BIOS provides for a thirty one second period for the HDD to respond with the "drive ID" information stored describing it. Accordingly if the security logic 326 is not able to provide the "drive ID" information within this time, from the time that the BIOS reaches the "drive ID" equipment check stage 69, for whatever reason, then the BIOS will indicate that the storage media 21 at that location is not functional and bypass it. As the security logic 326 in south bridge 312 is expected to be well and truly initialised and operational by this time, such a delay would generally be indicative that there is indeed a problem with the protected HDD(s).

After supplying the host CPU 13 with the "drive ID", the security logic 326 in south bridge 312 advances to its next state, still blocking data communications between the host CPU 13 and the protected storage media 21, whilst the BIOS program proceeds with its normal boot up procedure at steps 71 through to 81, until it arrives at step 81 involving loading of a valid boot sector.

During this state, the security logic 326 in south bridge 312 waits for a boot sector request from the host CPU 13 to the IDE interface logic 31. On receiving the BIOS request, instead of loading the boot sector stored on the protected storage device, the security logic 326supplies a "custom" boot sector stored in invisible HDD partition 330to the host CPU 13 as indicated by step 107. The CPU 13 then runs the boot loader according to the custom boot sector, which causes a prescribed authentication application program stored within the invisible HDD partition 330 to be loaded at step 109 and then executed at step 111. Similar to the application program and user profiles, the custom boot sector and prescribed authentication application program may alternatively be stored in south bridge 312 itself or in a separate secure memory connected to south bridge 312.

In the present embodiment, the valid boot sector must be that which is stored on the protected storage media 21; otherwise the security logic 326 in south bridge 312 never advances beyond its blocking state. Such an arrangement ensures the integrity of the security of the system by not allowing any external operating system, other than that which is provided on the protected storage media 21, to effect control of the host CPU 13 for the purposes of communicating with data stored on the protected storage media 21.

Thus, in the normal operation of the computer system, where the BIOS targets the protected storage media 21 for the purposes of locating and loading the boot sector, the BIOS causes the host CPU 13 to request the boot sector from the protected storage media 21.

The authentication application program essentially comprises a prescribed login application that only allows an authenticated user to continue with operation of the computer system 11. A user that is unable to be authenticated by the prescribed

login application cannot continue to use the computer system. The detailed operation of the login application will be described in more detail later, but for the purpose of describing the system start up sequence, will be described in general terms.

Moreover, the login application requires the user to enter a valid login name and password for the computer system to progress beyond the initial login stage. The login application in the present embodiment is designed to allow only three attempts at entering the correct login name and password. It should be appreciated that in other embodiments the number of login attempts that may be allowed can be different, and in extreme security applications, may be limited to just one attempt. If the correct login name and password are not entered by the third attempt, the application program invokes a system halt (wherein the system hangs or loops indefinitely), which requires the entire cold boot process to be repeated.

Valid login names and passwords associated therewith for all users permitted access to the storage media 21 are stored in the invisible HDD partition 330. Alternatively, they can be stored in south bridge 312 itself or in a separate secure memory connected to south bridge 312. Accordingly, various communications proceed during this login phase between host CPU 13 under the control of the authentication application program and the security logic 326 in south bridge 312 as shown at 112.

If the login is successful, as represented by step 113, the authentication application program proceeds in a manner to be described in more detail later. With respect to the security logic 326 in south bridge 312, once the user has been authenticated, the data access profile previously stored for that particular user in the invisible HDD partition 330 is set at 114 to determine the protocol of operation between the authentication application program and the operating system of the security logic 326 thereafter. During this phase of operation, the security logic 326 passes details of the data access profile of the particular user to the host CPU 13 for display. Depending upon the access level of the user, possibly login and password information as well as data access profile information of other users

having access to the storage media 21 are passed over to the host CPU 13 for display and possible editing under the authentication application program.

This phase of operation continues until the user invokes an "allow boot" process at step 115. Setting this status causes the security logic 326 in south bridge 312 to enter the second phase of its operation at step 117. At this stage, the operating system being run by the security logic 326 sets the data access profile of the authenticated user at step 119, which profile is thereafter enforced for determining the host CPU 13 access to the protected data storage media 21.

The operating system of the security logic 326 then signals the authentication application program run by the host CPU 13 at 120 that the security logic 326 is configured to adopt the data access profile of the user, whereupon the application program at 121 issues the software interrupt vector to the host CPU 13 invoking a "warm boot". The appropriate soft boot vector is then loaded and the host CPU 13 causes a soft system re-start or warm boot at step 85.

During the software reset, the security logic 326 then enters a waiting state for the boot sector request as indicated at 123, whilst enforcing the data access profile for all data communications between the host CPU 13 and the protected storage media 21 as shown at 125. Importantly, whilst the computer system 11 is undergoing the system reset, security logic 326 still remains active and fully operational during this time.

A software reset "warm boot" invokes a special subroutine of the BIOS program that performs an abbreviated start up sequence. Moreover, essentially steps 51 to 63 are bypassed and the BIOS program proceeds with operation at about step 65.

At step 69, which invokes the equipment check involving the "drive ID" with respect to the HDD, the operating system of the security logic 326 in south bridge 312 no longer intercepts the request from the host CPU 13 to the protected storage media 21, as long as the access to the HDD of the storage media is in conformance with the particular user data access profile that has been set by the

operation of the security logic 326 during the first phase of its operation. Such access will be permitted in most cases, unless the administrator has specifically barred the authenticated user from HDD access.

Thus, the security logic 326 in south bridge 312 allows the HDD of the storage media 21 to respond directly to the request with the "drive ID", whereupon the host CPU 13 advances the BIOS program through steps 71 to 81, in accordance with the normal boot up sequence of the BIOS.

Importantly, the initial part of the data access profile enforcement process involves the operating system of the security logic 326 blocking access to the protected storage media 21 until a valid BIOS boot sector request is detected from the host CPU 13 via the ATA cable 33. Importantly, the security logic rejects all other commands to the protected storage media during step 125.

On the BIOS requesting a boot sector from the particular HDD of the protected storage media 21, the security logic 326 allows the request to proceed.

On the BIOS receiving a valid signature from the storage media, the host CPU 13 then proceeds with loading the prescribed boot sector from the storage media 21 at step 81 and proceeds running the boot loader to load the operating system from the storage media 21 at step 83, in accordance with the normal operation of the computer system.

Following receipt of a valid BIOS request for the boot sector on the storage media 21, the security logic 326 in south bridge 312 then adopts a monitoring state of all media channel activity along the ATA cable 33 according to the set data access profile of the authenticated user as indicated at 127. Accordingly, the security logic 326 only allows or disallows access to relevant partitions and files within the storage media 21 in conformance with the set user data access profile, whereby data that the user is not permitted to access cannot be accessed by the user or by any virus, errant application program or unauthorised access.

The security logic 326 maintains this monitoring or supervisory state until the computer system 11 is shutdown and powered off. Once power is switched off to computer system 11, all dynamic memory is erased and access to the storage media is barred until the device is powered up and initialised again.

Now having described the overall operation of the security logic 326 in south bridge 312, the authentication application program will now be described in more detail with respect to the flow chart shown in Figure 8 and the GUI screen graphical specification formats as shown in Figures 9A through to 9E.

The user authentication application program, on being loaded by the boot loader at step 109 and run by the host CPU at step 111, commences at 130 and initially causes a user login screen to be displayed at step 131, the graphical specification for which is shown at Figure 9A of the drawings. The screen 132 is divided into a heading frame 133, a login frame 135 and a message/log frame 137.

The heading frame 133 has provision for the product trade mark at 139, the version number at 141, the screen name at 143 and provision for display of legal warning notices at 145.

The login frame 135 includes banners for the text "user:" at 147 and the text "password:" 149, with frames for respectively entering the user identification or "user ID" at 151 and the user password at 153. The message/log frame comprises a banner for displaying the text "messages" at 157 and a message frame 159, which displays status messages issued by the security logic to the authentication application program as a scrollable list. A login button 155 is also provided in order for the user to invoke the processing of the user and password entries for authentication purposes by the security logic 326 in south bridge 312.

Whilst the screen 132 is displayed, the application program waits for the login ID and password to be entered as shown at step 160. Activating the login button 155 involves the authentication application program invoking a process at 161 causing the host CPU 13 to pass the login details entered on the screen to the security logic 326 in south bridge 312, whereupon the security logic 326 compares the

received login information with stored login information provided in the invisible HDD partition 330. Depending upon whether there is a valid match between the entered user and password information via the login screen and the stored user and password information, the security logic 326 returns either a valid or invalid authentication signal to the host CPU 13.

In the case of there being a valid authentication as shown at 162, the security logic 326 also provides additional information concerning the user type and associated device information depending upon the stored data access profile of the particular user.

In the case of there being an invalid authentication, a counter 324 is incremented/decremented to record that a first unsuccessful attempt at authentication has been made and an appropriate message is displayed to the user on the message/log frame 137, indicating the failed status of the authentication attempt as shown at 163. As previously described, on three unsuccessful authentication attempts as shown at 164, the authentication application program causes a shutdown interrupt vector to be invoked by the host CPU 13 at 165, resulting in a complete shutdown of the computer system 11 requiring a cold boot to restart the system.

On valid authentication, the authentication application program then proceeds at 166 with displaying one of either two types of login screen, depending upon the user type. In the present embodiment, there are two user types, one being a normal user, for which the screen as shown by the graphical specification at Figure 9B is displayed at step 167, and the other being an administrator for which the screen represented by the graphical specification at Figure 9C is displayed at step 168.

The graphical specification for the normal user GUI screen 169 is generally divided into a heading frame 170, a login details frame 171, a device details frame 172 and a message/log frame 173. The screen also includes a launch system button 174 that will be further described.

The heading frame 170 is essentially the same as the heading frame 133 for the general login screen, where the same reference numerals have been used to identify corresponding attributes of the frame. In this case, however, the screen title is modified to represent that it is a user type login screen, as shown at 143 of the drawings.

The login details frame 171 is similar to the login frame 147 of the preceding screen and accordingly the same reference numerals have been used to identify corresponding attributes of the frame. The login details frame, however, includes a user ID display frame 175 to display the user ID as opposed to an entry frame in the proceeding screen. The login details frame also includes a new password accept button 176, which is used in conjunction with the password entry frame 153 to permit the user to change its password. Accordingly, activating the new password button 176 invokes a process within the authentication application program involving communication between the host CPU 13 and the security logic 326 in south bridge 312 to cause a change to the password stored within the invisible HDD partition 330 for the particular user as shown at 177. A standard routine involving confirmation of the new password is adopted, before the password changes are completed.

The device details frame 172 includes a title banner 178, which displays the text "device information", as well as two further sub-banners displaying the text "master" at 179 and "slave" at 181. These sub-banners head regions for displaying information about the prescribed device or devices that are protected by the security logic 326 in south bridge 312. In the present embodiment, up to two storage devices are allowed, which is normal under the ATA standard, one being denoted the "master" device and the other being denoted the "slave" device. The respective regions detailing the device information include three further sub-level banners for displaying the text "device" at 183, "access" at 185 and "size MB" at 187. Display frames 189 for each sub-banner are respectively provided below the device, access and size banners for listing the device details that the user is permitted to observe on the master and/or slave device, as set by the administrator.

For each observable device, the list displays:

- the device number;
- its access type for the user: and
- the device size in MB (MegaBytes).

The access type lists one of five possible designations:

- read only, which is displayed in red text;
- read/write, which is displayed in green text;
- invisible, which is displayed in yellow text;
- read directory entry, which is displayed in grey text; and
- delete, which is displayed in blue text.

The message/log frame 173 includes a title banner 157 for displaying the text "messages" and a display frame 159, which displays status messages provided by the security logic as a scrollable list, similar to the preceding screen.

In the case of the user, the device information is only provided for display purposes and cannot be changed.

Now explaining the methodology behind the listings contained in the display frames 189 and the action provided thereby in more detail, in the present embodiment, the protected storage device is divided into zones or partitions that have different access level permissions depending upon the determination of the administrator. These partitions can be created in a known manner and are represented as separate devices for each type of storage device. For example, these partitions may comprise C:, D:, E: and F:. Thus, each user can have one of five types of access to these partitions, namely read only, read/write, invisible, read directory entry and delete.

Read only access means that the user can access all of the files existing in the designated partition, but can only read the file contents. The user has no write or delete permissions with respect to the files in that partition.

Read/write access means that the user can access all of the files existing in the designated partition and perform both read and write functions with respect to the file contents, but has no delete permissions with respect to those files.

Invisible access means that none of the files within the designated partition are accessible to the user in any form and are hidden, even to the extent that no file details can be listed or be visible at all in any directory listing of files for that partition available to the user.

Read directory entry access means that the user may be able to list file details such as names and attributes in any directory listing of files in the designated partition, but the user has no read, write or delete permissions in relation to any of the files in that partition.

Delete access is the highest level of access to any files within a designated partition, whereby the user not only has full read and write permissions, but also delete permissions in relation to all of the files in that partition.

When the user is ready to continue on with operation of the computer system 11, the launch system button 174 is activated as shown at 190, whereupon the authentication application program sends a signal to the security logic 326 in south bridge 312 to set the "allow boot" status therein as by step 191. Setting the "allow boot" status invokes the commencement of the second phase of operation of the security logic 326, as shown at step 117, allowing the system start up sequence to continue with the authentication application issuing a "warm boot" interrupt vector as step 120 in the manner as previously described. This halts the operation of the user authentication application program.

In the case of the user type being an administrator, the administrator screen as represented by the graphical specification shown in Figure 9C is displayed to the

user on the monitor via the authentication application program at step 168. The administrator type screen 192 is substantially similar to the user type screen and so the same reference numerals have been used to identify corresponding attributes between the two screens. Accordingly, the administrator type screen is divided into a similar heading frame 193, login details 195, device details frame 197 and a message/log frame 199.

With respect to the banner title 143 of the heading frame 193, the text is altered to indicate that the screen is for the administrator type login.

The device details frame 197 and the message/log frame 199 are substantially identical to the corresponding attributes of the user type screen and will not be described further. The launch system button 174 functions in an identical manner to the launch system button of the preceding screen, whereby activation of the same as shown at 200 invokes the commencement of the second phase of operation of the security logic 326 in south bridge 312 as previously described.

With the login details frame 195, the same facility for changing the password of the administrator is provided as shown at step 201, with a similar entry frame 153 and accept new password button 176, as in the case of the user type login. However, the login details frame also includes an edit users button 202, activation of which invokes an editing process within the authentication application program as shown at 203, allowing the administrator to create and edit data access profiles for individual users, so as to determine their data access profile for permitted access to the storage media 21. Activation of the button 201 causes the authentication application program to display at 204 an administrator editing screen to the user, the graphical specification of which is shown at Figure 9D of the drawings.

The administrator users edit screen 205 is divided into a heading frame 206, an edit user details frame 207, a message/log frame 209 and a return to admin login button 211. The heading frame 206, apart from having an appropriately worded title banner 143 denoting the screen as being an administrator edit users screen is identical to previous heading frames. Similarly, the message/log frame 209 is

substantially identical to the message/log frame with the proceeding screens. Thus the same reference numerals have been used to identify corresponding attributes of each of these screens.

With respect to the edit users details frame 207, this comprises a title banner depicting the text "user list" as shown at 213 and sub-title banners depicting the text "user" at 215, "password" at 217 and "access" at 219. An editable frame 221 is provided below the sub-banners in which is displayed a scrollable and editable list of all users having access to the protected storage media 21. This list is derived from data stored within the invisible HDD partition 330 arising from communications between the host CPU 13, under the control of the authentication application program, and the security logic 326, under the control of the operating system thereof.

Each user entry in the list contains:

- the user ID;
- password; and
- access button;

under the respective sub-title banners 215, 217 and 219.

Upon pressing the access button for a particular user, the access edit screen will appear for that user. The administrator editing process allows a user to be deleted by the administrator through the edit frame 221 by selecting their entry and pressing the ALT-d key sequence on the keyboard.

A create new user button 223 is also included within the edit user details frame 207 for creating a new user. Activation of the button 223 invokes a prescribed process within the authentication application program as shown at 224. This process causes a dialogue box to be displayed over the administrator edit users screen 205 providing for frames for entering the user ID and password, and an accept button, whereupon activation of which causes the user and password to be displayed in the edit frame 221 as shown at 225. Each new user has an initial

default data access profile, which sets up all partition devices as hidden, until such time as the administrator edits the data access profile for the user using the access edit screen. The administrator accesses this screen by activating the corresponding access button as shown at 226 for the user requiring editing in the edit frame 221.

The return to admin login button 211 is provided to allow the administrator to return to the administrator type login screen 191 from the administrator edit users screen 205 as shown at 227.

Activating the access button beneath the sub-title banner 219 alongside any user listed in the user list of the edit user details frame 207 causes the authentication application program to display at step 228 the administrator access edit screen, the graphical specification of which is shown in Figure 9E of the drawings. The administrator access edit screen 229 is divided into a heading frame 230 and an edit access details frame 231, a message/log frame 232 and a return to admin user text edit screen button 233.

The heading frame 230 is the same as in preceding screens except that the title banner is provided with appropriate text to identify that the screen is of the administrator access edit type as shown at 235. The message/log frame 232 is the same as in proceeding screens and accordingly the same reference numerals have been used to identify corresponding attributes between the screens.

The edit access details frame 231 comprises a head banner 235 displaying the text "access details", a sub-banner 237 containing the text "user" and a display frame 239 adjacent thereto for displaying the user ID of the particular user selected from the administrator edit user screen 205.

The edit access details frame 229 then provides a similar frame set up to the device frames of the user type login screen 169 and the administrator type login screen 192, whereby banners for the "master" and "slave" storage media protected by the security logic 326 provided at 179 and 181 and respective sub-

title banners 183, 185 and 187 detailing the "device", "access" and "size (MB)" titles respectively are provided for each device.

Device detail frames 239 are provided below each of these sub-title banners similar to the display frames 189 of the device detail frames 172 and 197 of the user login and administrator login screens respectively. The device detail frames 239, however, are editable, whereas the former two were not. Accordingly, each device details frame lists the device number under the sub-title banner 183, the access type for the user under the sub-title banner 185 and the device size in MB under the size (MB) sub-title banner 187.

The access type for the user is divided into five types:

- read only, depicted in red text;
- read/write, depicted in green text; and
- invisible, depicted in yellow text;
- read directory entry, depicted in grey text; and
- delete, depicted in blue text.

As in the previous case, the device numbers represent each of the partitions that are created for the particular storage media device. This, together with the size information, is display only, as determined by the information prescribed for the particular partition stored within the invisible HDD partition 330, whereas the access type is editable by highlighting and clicking the displayed entry. In this respect, the displayed entries cycle between read only, read/write, invisible, read directory entry and delete through the graphical user interface by clicking an invisible frame around the displayed text.

In this manner, the access type for each partition can be individually set and edited to create a particular data access profile for the selected user. The particular data access profile created for the user is processed by the

authentication application program and supplied to the security logic 326 in south bridge 312 on activating the return to admin user edit screen button 233 as shown at 241. At this time, the display data access profile as determined by the administrator is communicated to the security logic 326 by the host CPU 13 and stored within the invisible HDD partition 330.

Simultaneously, the authentication application program returns to displaying the administrator edit user screen 205 from which the administrator can select and edit the data access profile of other users in the edit list 207.

The second embodiment of the invention is substantially similar to the first embodiment, except that the security system is implemented in a bus bridge integrated circuit (IC) provided on the HDD. This embodiment arises from developments with the serial ATA (SATA) standard for connecting HDD's into computer systems.

As a consequence of the design of SATA interfaces bus bridge IC's have been developed in the form of a highly integrated System-On-Chip (SOC) device, an example of which has been recently announced by Infineon Technologies. This SOC device integrates a 1.6 Gbit/s read channel core, a 3 Gbit/s native SATA interface, a 16-bit microcontroller, a hard disk controller, embedded memory and a quality monitoring system. Such a device is designed to be incorporated into the control circuit of a HDD, essentially bridging communications between a computer bus using a SATA channel for communicating with a storage device, and the HDD of the storage device.

In the present embodiment, the security system is incorporated into a bus bridge circuit of similar configuration to the SOC device described above and has application software operating the same stored on a HDD to which the bus bridge circuit is connected.

As shown in Figure 10, the bus bridge circuit 351 comprises a CPU 353, having memory RAM 355, a SATA interface 357, a disk controller interface 359 and security logic 361.

As in the preceding embodiment, the security logic 361 of the bus bridge circuit 351 is configured to load application software stored on the HDD into RAM 355 to selectively secure accesses between the main computer and the HDD, in conjunction with the normal operation of the disk controller.

The function of the application software is substantially identical to that described in relation to the preceding embodiment except for the fact that the security system is interfaced with and integrated into the hardware and firmware design of the SOC device to exercise control over disk accesses using the disk controller functionally of the device itself.

As the security system functionality is identical to that described in the preceding embodiment, it will not be described again.

Now having described the function and the various processes performed by the computer system and the security system with regard to the two embodiments, it can be seen that the subject invention has several distinguishing and advantageous attributes and features compared with known prior art systems.

In particular it should be appreciated that the security logic (326/361) itself described in the specific embodiments is physically disposed in bus bridge circuitry (312/351) and connected solely to the data access channel between the computer system and the interface logic communicating with the main CPU data and address bus 15 and the storage media 21. The two embodiments themselves are distinguished by the relative location of the bus bridge circuitry, relative to the type of communication standard being employed, and the opportunity of integrating the security system physically within the south bridge 312 on the motherboard or I/O board, or the SOC disk drive controller 351 on the HDD itself. Importantly, in either case, the security logic (326/361) is not connected directly to the main bus 15, thereby preventing any opportunity of the device to act as an addressable device and be over-ridden by the operation of the host CPU 13.

Furthermore, being confined to communicating with the storage media at either end of the data access channel and the more generic standardisation of such access channels compared with main bus structures of computer systems, increases the utility of the security logic in bus bridge circuitry for use with a large number of different types of computer systems which may have varying bus structures but utilise the same data access channel standard. In this respect, there are only a few common types of data access channel, ATA, SATA, SCSI, fibre, USB etc, whereas the diversity and complexity of bus structures are far more widespread.

Another attribute of the present embodiment is that the security logic in the bus bridge circuitry still intercepts communication with the protected data storage media at the earliest possible stage in the computer start up sequence and is entirely self-contained and connected in as part of the computer system's own circuitry.

As discussed in WO 03/003242, other types of data storage protection devices and anti-virus systems are not entirely self-contained, requiring set up by inserting a separate floppy disk, CD ROM, or other way of installing software onto the host computer, which is not accessed until well into the BIOS program after performance of the "device ID", where the storage device is vulnerable to unauthorised access, or even well after the installation of the operating system files. In particular, when compared with software protection systems, which tend to be the main type of anti-virus protection system being promoted at present, the operating system of the computer needs to be loaded before the application program can be run, which provides huge openings for unauthorised access to the storage device as can be seen from the aforementioned description, before any type of protection can be provided by the anti-virus application program.

It should be also appreciated that the particular configuration of the security logic in bus bridge circuitry provides for extendibility, allowing for other types of storage media 47 to be connected thereto via a custom interface 49 and secure media interface 45.

It should be appreciated that the scope of the present invention is not limited to the particular embodiments herein described and that other embodiments of the invention may be envisaged without departing from the scope or spirit of the present invention. For example, the bridging and system functions of the south bridge and north bridge may be integrated into a single chip. The present invention is not restricted to south bridge computer architectures but may apply to any other bus bridging architectures as demonstrated in the second embodiment.

The Claims Defining the Invention are as Follows

1. A security system for a computer having a host central processing unit (CPU), memory used by the host CPU to load programs in order to operate the computer, a storage device for storing data to be handled by the computer, and a bridge circuit interposed between a first bus connected to the host CPU and a second bus connected to the storage device, the security system comprising:

   processing means independent of the host CPU for controlling access between the host CPU and the storage device; and

   program memory means independent of the memory of the computer to unalterably store and provide computer programs for operating the processing means in a prescribed manner to control said access;

   wherein the processing means comprises logic in the bridge circuit.

2. A security system as claimed in claim 1, including memory store means independent of the memory means of the computer to store critical data and control elements associated with the basic operation of the computer and access to the storage device.

3. A security system as claimed in claim 1 or 2, wherein the memory store means is connected to or included in the bridge circuit.

4. A security system as claimed in any one of the preceding claims, wherein said critical data and control elements are supplied to and used by the host CPU for verification of the storage device and operating the computer independently of the storage device during the start up sequence of the computer.

5. A security system as claimed in any one of the preceding claims, further comprising authentication means to authenticate a user of the computer having a prescribed profile of access to the storage device.

6. A security system as claimed in claim 5, wherein the authentication means comprises logic in the bridge circuit.

7. A security system as claimed in claim 5 or 6, wherein the authentication means includes a login verifying means to enable a user of the computer to enter a login identification and password and have that login identification and password verified to authenticate said user being an authorised user of the computer having a prescribed profile of access to the storage device before allowing the start up sequence of the computer to proceed further.

8. A security system as claimed in claim 7, wherein said login identification and passwords of authorised users and said prescribed profile of access thereof form part of said critical data and control elements and said login verifying means accesses said critical data and control elements to effect authentication of a user.

9. A security system as claimed in claim 7 or 8, wherein said prescribed profile of access comprises a prescribed allocation of predetermined levels of access permitted for an authorised user of the computer to prescribed partitions or zones of the storage device.

10. A security system as claimed in any one of the preceding claims, including intercepting means to block all data access by the host CPU to the data storage device before initialisation of the security system and intercept all said data access immediately after said initialisation under the control of said processing means.

11. A security system as claimed in claim 10, wherein the intercepting means comprises logic in the bridge circuit.

12. A method for securing and protecting a storage device for storing data to be handled by a computer from unauthorised access, the computer having a host central processing unit (CPU), memory used by the host CPU to load programs in order to operate the computer and storage device, and a bridge circuit interposed between a first bus connected to the host CPU and a second bus connected to the storage device, the method comprising:-

controlling access between the host CPU and the storage device independently of the host CPU using logic in the bridge circuit; and

unalterably storing computer programs for effecting said controlling access in a location separate from the memory and not addressable by the host CPU.

13. A method as claimed in claim 12, including storing critical data and control elements associated with the basic operation of the computer and access to the storage device in a location separate from the memory and not addressable by the host CPU.

14. A method as claimed in claim 13, including storing the critical data and control elements in memory store means connected to the bridge circuit.

15. A method as claimed in claim 13, including storing the critical data and control elements in the bridge circuit.

16. A method as claimed in any one of claims 13 to 15, including independently supplying the host CPU with said critical data and control elements for verification of the storage device and operating the computer independently of the storage device during the start up sequence of the computer.

17. A method as claimed in any one of claims 12 to 16, including authenticating a user of the computer having a prescribed profile of access to the storage device.

18. A method as claimed in claim 17, wherein said authenticating includes enabling a user of the computer to enter a login identification and password and verifying the same to establish whether the user is an authorised user of the computer having a prescribed profile of access to the storage device before allowing the start up sequence of the computer to proceed further.

19. A method as claimed in claim 18, wherein said login identification and passwords of authorised users and the prescribed profile of access thereof form part of said critical data and control elements and the verifying includes comparing the entered login identification and password with the login identification and passwords within said critical data and control elements and authenticating a user if there is match.

20. A method as claimed in any one of claims 17 to 19, wherein the prescribed profile of access comprises a prescribed allocation of predetermined levels of access permitted for an authorised user to prescribed partitions or zones of the storage device.

21. A method as claimed in any one of claims 12 to 20, including blocking all data access by the host CPU to the data storage device during initialisation of the computer and intercepting all said data access during the start up sequence after said initialisation.

22. A method as claimed in any one of claims 12 to 21, as dependent on claim 13, wherein said critical data and control elements include identification data in respect of the storage device for enabling the computer to complete its peripheral check during said start up sequence.

23. A method as claimed in any one of claims 12 to 22, as dependent on claim 13, wherein said critical data and control elements include a custom boot sector for the computer that includes invoking the authenticating step; and the method includes assuming operation of the computer during said start up sequence with the custom boot sector and authenticating the user of the computer at such time.

24. A method as claimed in any of claims 12 to 23, as dependent on claim 17, wherein said authenticating includes enabling a particular prescribed level of authorised user to create and edit login identifications and passwords within the critical data and control elements for specifying authorised users having access to the storage device.

25. A method as claimed in any of claims 12 to 24, as dependent on claim 17, wherein said authenticating includes enabling a particular prescribed level of authorised user to create and edit login identifications and passwords within the critical data and control elements for specifying authorised users having access to the storage device.

26. A method as claimed in any one of claims 12 to 25, as dependent on claim 17, wherein said authenticating of a user is performed only in the bridge circuit.

27. A security system for a computer having a host central processing unit (CPU), memory used by the host CPU to load programs in order to operate the computer, a storage device for storing data to be handled by the computer, and a bridge circuit interposed between a first bus connected to the host CPU and a second bus connected to the storage device, the security system comprising:

processing means independent of the host CPU for controlling access between the host CPU and the storage device; and

intercepting means to block all data access by the host CPU to the data storage device before initialisation of the security system and intercept all said data access immediately after said initialisation under the control of said processing means;

wherein said processing means effects independent control of the host CPU and configuration of the computer in a manner so as to prevent unauthorised access to the storage device on said intercepting means intercepting said data access immediately after said initialisation; and

wherein the processing means and intercepting means comprise logic in the bridge circuit.

28. A security system as claimed in claim 27, including program memory means independent of the memory of the computer to unalterably store and provide computer programs for operating the processing means in a prescribed manner to control said access.

29. A security system as claimed in claim 28, wherein the program memory means is connected to or included in the bridge circuit.

30. A security system as claimed in any one of claims 27 to 29, further comprising authentication means to authenticate a user of the computer having a prescribed profile of access to the storage device.

31. A security system as claimed in claim 30, wherein said prescribed profile of access comprises a prescribed allocation of predetermined levels of access permitted for an authorised user of the computer to prescribed partitions or zones of the storage device.

32. A security system as claimed in any one of claims 27 to 31, wherein said bridge circuit is adapted to be connected only in line with the data access channel between the host CPU and the storage device, and off the main data and control bus of the host CPU.

33. A method for securing and protecting a storage device for storing data to be handled by a computer from unauthorised access, the computer having a host central processing unit (CPU), memory used by the host CPU to load programs in order to operate the computer and storage device, and a bridge circuit interposed between a first bus connected to the host CPU and a second bus connected to the storage device, the method comprising:-

controlling all data access between the host CPU and the storage device independently of the host CPU;

blocking all data access by the host CPU to the storage device during initialisation of the computer; and

intercepting all said data access during the start up sequence after said initialisation to effect independent control of the host CPU and configuration of the computer in a manner so as to prevent unauthorised access to the storage device thereafter;

wherein all data access is controlled, blocked and intercepted by logic in the bridge circuit.

34. A method as claimed in claim 33, including unalterably storing computer programs for effecting said controlling access in a location separate from the memory and not addressable by the host CPU.

35. A method as claimed in claim 33 or 34, including unalterably storing computer programs for effecting said controlling access in memory store means connected to the bridge circuit.

36. A method as claimed in claim 33 or 34, including unalterably storing computer programs for effecting said controlling access in the bridge circuit.

37. A method as claimed in any one of claims 33 to 36, including authenticating a user of the computer having a prescribed profile of access to the storage device.

38. A method as claimed in claim 37, wherein said authenticating includes enabling a user of the computer to enter a login identification and password and verifying the same to establish whether the user is an authorised user of the computer having a prescribed profile of access to the storage device before allowing the start up sequence of the computer to proceed further.

39. A method as claimed in claim 38, wherein said login identification and passwords of authorised users and the prescribed profile of access thereof form part of said critical data and control elements and the verifying includes comparing the entered login identification and password with the login identification and passwords within said critical data and control elements and authenticating a user if there is match.

40. A method as claimed in any one of claims 37 to 39, wherein said prescribed profile of access comprises a prescribed allocation of predetermined levels of access permitted for an authorised user to prescribed partitions or zones of the storage device.

41. A method as claimed in any one of claims 37 to 40, wherein said authenticating of a user is performed only in said bridge circuit.

42. A security system for a computer having a host central processing unit (CPU), memory used by the host CPU to load programs in order to operate the computer, a storage device for storing data to be handled by the computer, and a bridge circuit interposed between a first bus connected to the host CPU and a second bus connected to the storage device, the security system comprising:

blocking means for selectively blocking data access between the host CPU and the storage device; and

authentication means to authenticate a user of the computer having a prescribed profile of access to the storage device;

wherein said blocking means maintains said blocking data access until said authentication means completes correct authentication of the user of the computer; and

wherein the blocking means comprises logic in the bridge circuit.

43. A security system as claimed in claim 42, including processing means independent of the host CPU for controlling the operation of said blocking means for blocking access between the host CPU and the storage device in response to said authentication means.

44. A security system as claimed in claim 43, wherein said processing means comprises logic in the bridge circuit.

45. A security system as claimed in claim 43 or 44, wherein said authentication means comprises logic in the bridge circuit.

46. A security system as claimed in any one of claims 43 to 45, wherein said blocking means blocks all data access by the host CPU to the data storage device before initialisation of the security system and includes intercepting means to intercept all said data access immediately after said initialisation under the control of said processing means.

47. A security system as claimed in any one of claims 43 to 46, wherein said processing means effects independent control of the host CPU and configuration of the computer in a manner so as to prevent unauthorised access to the storage device, upon said intercepting means intercepting said data access immediately after said initialisation and before loading of the operating system of the computer.

48. A security system as claimed in any one of claims 43 to 47, wherein said authentication means enables a software boot of the computer to be effected after correct authentication of the user, and said processing means permits normal loading of the operating system during the start up sequence of the computer following said software boot.

49. A security system as claimed in any one of claims 43 to 48, wherein said processing means controls said blocking means to effect blocking access to the storage device after correct authentication of the user in accordance with the prescribed profile of access of the user.

50. A security system as claimed in any one of claims 43 to 49, including program memory means independent of the memory of the computer to unalterably store and provide computer programs for operating the processing means in a prescribed manner to control said access.

51. A security system as claimed in claim 50, wherein said program memory means is connected to or included in the bridge circuit.

52. A security system as claimed in any one of claims 43 to 51, including memory store means independent of the memory means of the computer to store critical data and control elements associated with the basic operation of the computer and access to the storage device.

53. A security system as claimed in claim 52, wherein said memory store means is connected to or included in the bridge circuit.

54. A method for securing and protecting a storage device for storing data to be handled by a computer from unauthorised access, the computer having a host central processing unit (CPU), memory used by the host CPU to load programs in order to operate the computer and storage device, and a bridge circuit interposed between a first bus connected to the host CPU and a second bus connected to the storage device, the method comprising:-

selectively blocking all data access between the host CPU and the storage device using logic in the bridge circuit; and

authenticating a user of the computer having a prescribed profile of access to the storage device;

wherein said blocking of data access is maintained until the user of the computer is correctly authenticated.

55. A method as claimed in claim 54, wherein said selective blocking comprises controlling access between the host CPU and the storage device independently of the host CPU.

56. A method as claimed in claim 54 or 55, wherein said selective blocking occurs during initialisation of the computer and includes intercepting all said data access during the start up sequence immediately after said initialisation and before loading of the operating system of the computer to enable independent control of the host CPU and configuration of the computer in a manner so as to prevent unauthorised access to the storage device.

57. A method as claimed in any one of claims 54 to 56, including performing a software boot of the computer after correct authentication of the user, and allowing normal loading of the operating system during the start up sequence of the computer thereafter.

58. A method as claimed in any one of claims 54 to 57, including controlling blocking access to the storage device after correct authentication of the user in accordance with the prescribed profile of access of the user.

59. A method as claimed in any one of claims 54 to 58, including unalterably storing computer programs for effecting said controlling access in a location separate from the memory and not addressable by the host CPU.

60. A method as claimed in claim 59, including unalterably storing computer programs for effecting said controlling access in memory store means connected to the bridge circuit. Preferably, the method includes unalterably storing computer programs for effecting said controlling access in the bridge circuit.

61. A method as claimed in any one of claims 54 to 60, wherein said authenticating includes enabling a user of the computer to enter a login identification and password and verifying the same to establish whether the user is an authorised user of the computer having a prescribed profile of

access to the storage device before allowing the start up sequence of the computer to proceed further.

62. A method as claimed in claim 61, wherein said login identification and passwords of authorised users and the prescribed profile of access thereof form part of said critical data and control elements and the verifying includes comparing the entered login identification and password with the login identification and passwords within said critical data and control elements and authenticating a user if there is match.

63. A method as claimed in any one of claims 54 to 62, wherein said prescribed profile of access comprises a prescribed allocation of predetermined levels of access permitted for an authorised user to prescribed partitions or zones of the storage device.

64. A method as claimed in any one of claims 54 to 63, wherein said authenticating of a user is performed only in the bridge circuit.

65. A bus bridge circuit for bridging data access between different buses or interfaces of a computer having a host CPU or a computer storage device, and for protecting unauthorised accesses of said computer storage device by said computer, the circuit comprising:

processing means for controlling operation of the circuit;

memory for loading application programs therein to be run by said processing means;

first interface means for interfacing the circuit with a first bus or device structure to communicate with the host CPU of the computer;

second interface means for interfacing the circuit with a second bus or device structure to communicate with the computer storage device; and

security logic means for controlling data access between said first interface means and said second interface means, in accordance with a prescribed application program run by said processing means, to prevent unauthorised data access to said computer storage device.

66. A bus bridge circuit as claimed in claim 65, wherein said prescribed application program is initially stored remotely of said bus bridge circuit in a hidden location within the storage device, and said security logic means is configured to load said application program into said memory means on setting of said bus bridge circuit.

67. A bus bridge circuit as claimed in claim 65 or 66, wherein said logic security means is configured to provide blocking means to block communications between said first interface means and said second interface means by default, and selectively allow controlled communications between said first interface means and said second interface means in accordance with said application software, after loading and running thereof by said processing means.

68. A bus bridge circuit as claimed in any one of claims 65 to 67, wherein said security logic means forms intercepting means to block all data access by the host CPU to the data storage device before initialisation of the bus bridge circuit and intercept all said data access immediately after said initialisation under the control of said processing means.

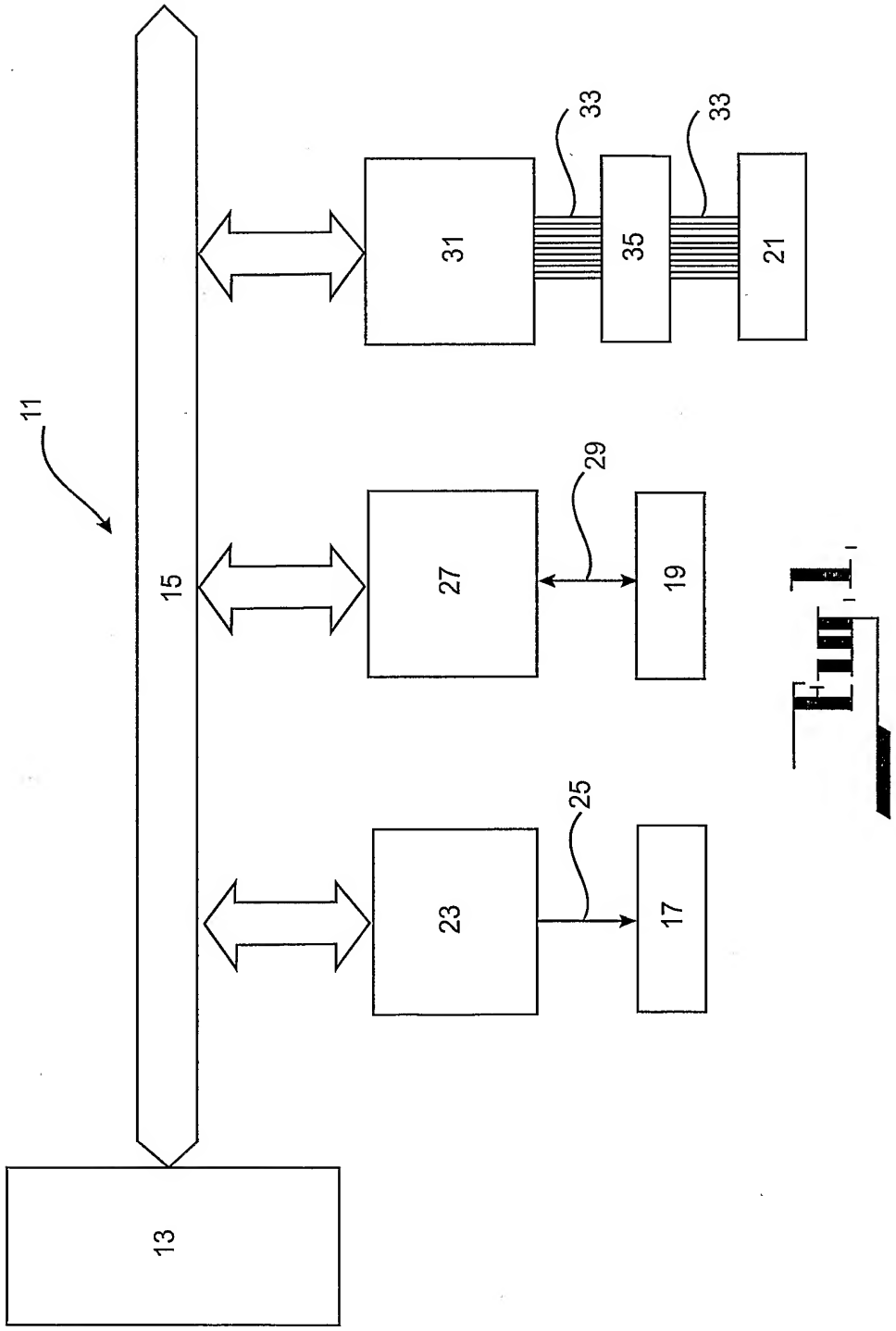
69. A bus bridge circuit as claimed in claim 68, wherein said prescribed software application provides for authentication means to authenticate a user of the computer having a prescribed profile of access to the storage device, and said blocking means maintains said blocking data access until said authentication means completes correct authentication of the user of the computer.

70. A security system for a computer substantially as herein described with reference to the accompanying drawings as appropriate.

71. A method for securing and protecting a storage device substantially as herein described with reference to the accompanying drawings.

72. A bus bridge circuit for bridging data access substantially as herein described with reference to the accompanying drawings.

5


11
15
13
31
33
35
33
21
27
29
19
23
25
17

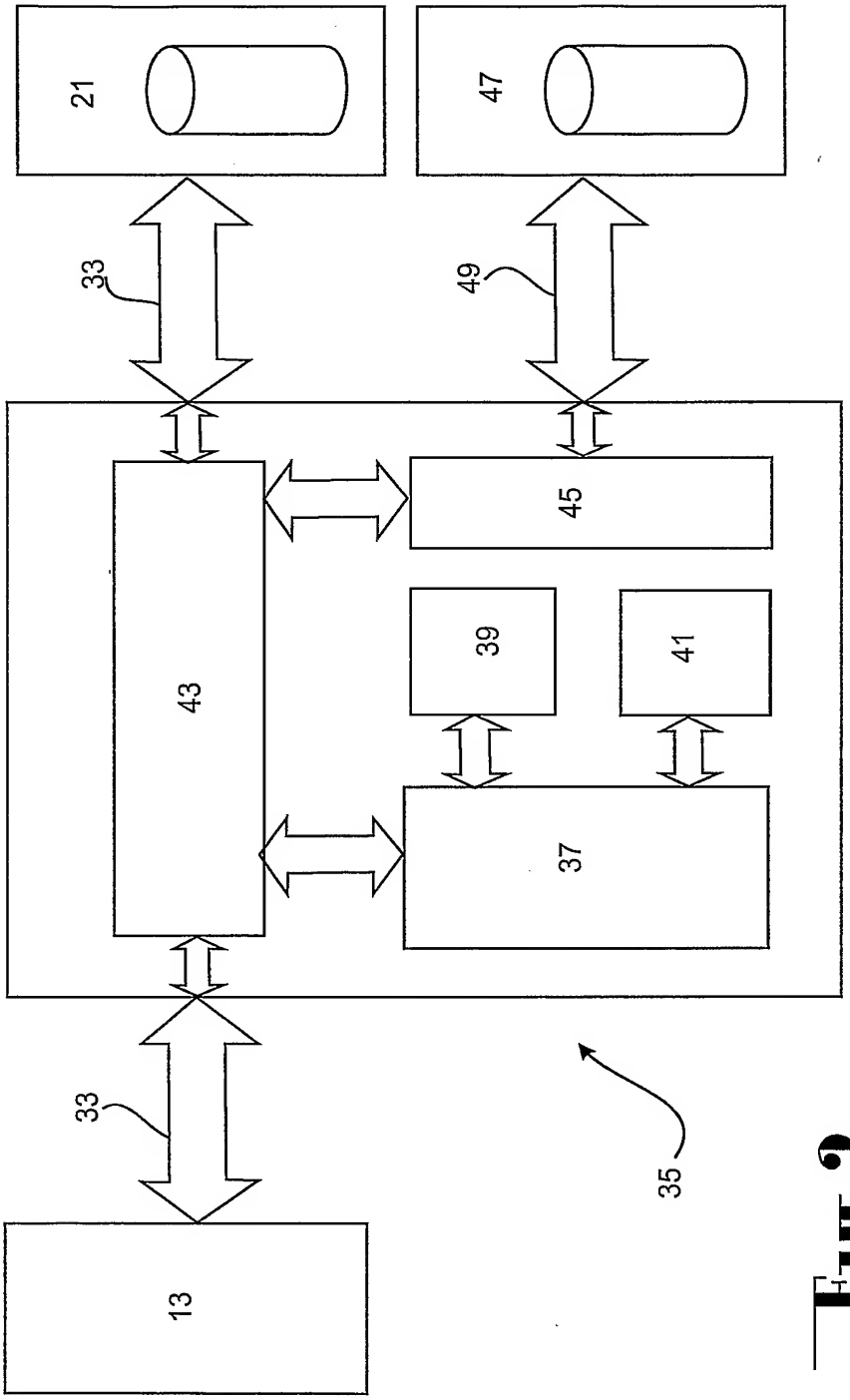


Fig. 2

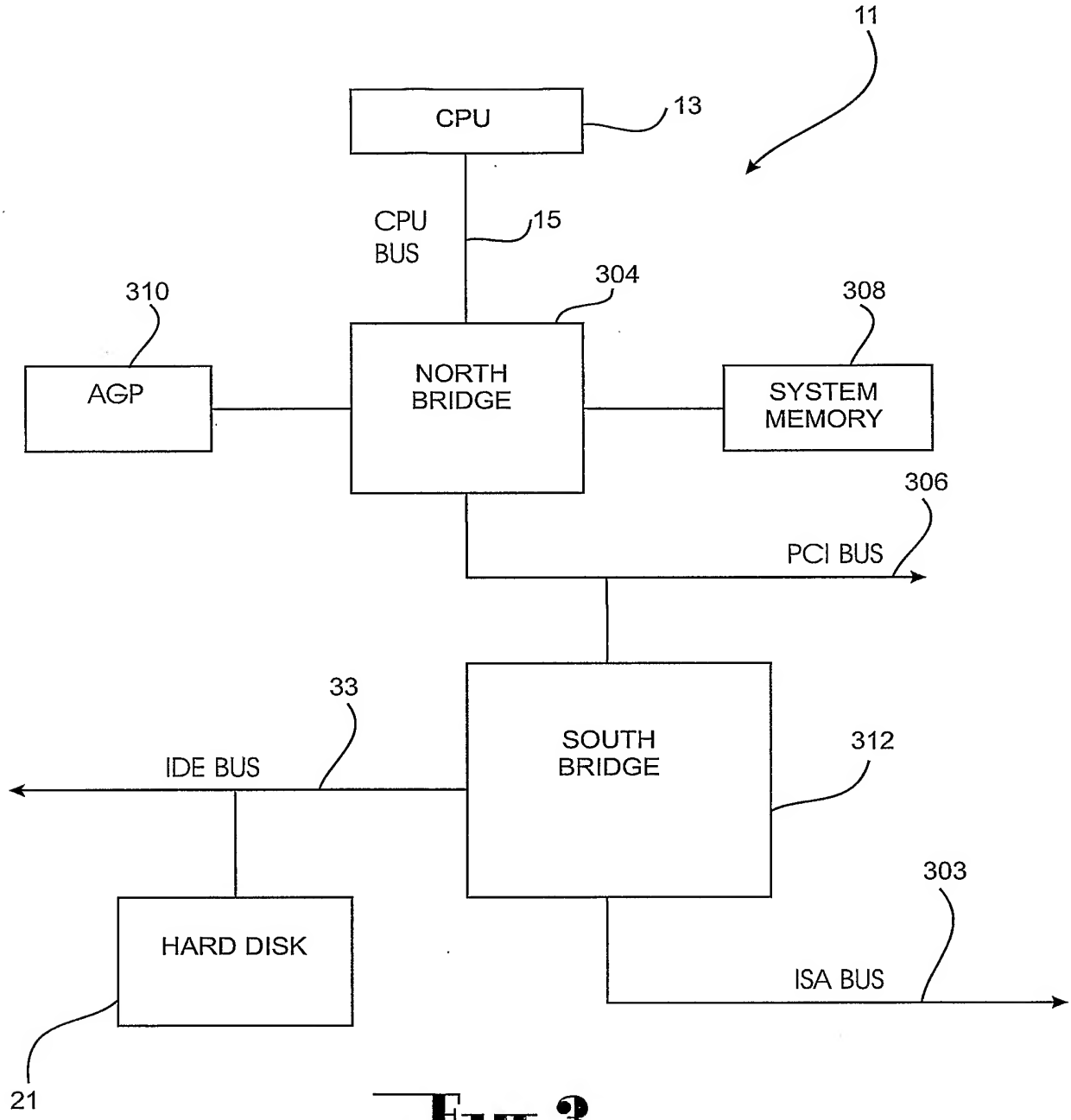

11
CPU
13
CPU
BUS
15
304
310
308
AGP
NORTH
BRIDGE
SYSTEM
MEMORY
306
PCI BUS
33
SOUTH
BRIDGE
312
IDE BUS
303
HARD DISK
ISA BUS
21

Fig. 3

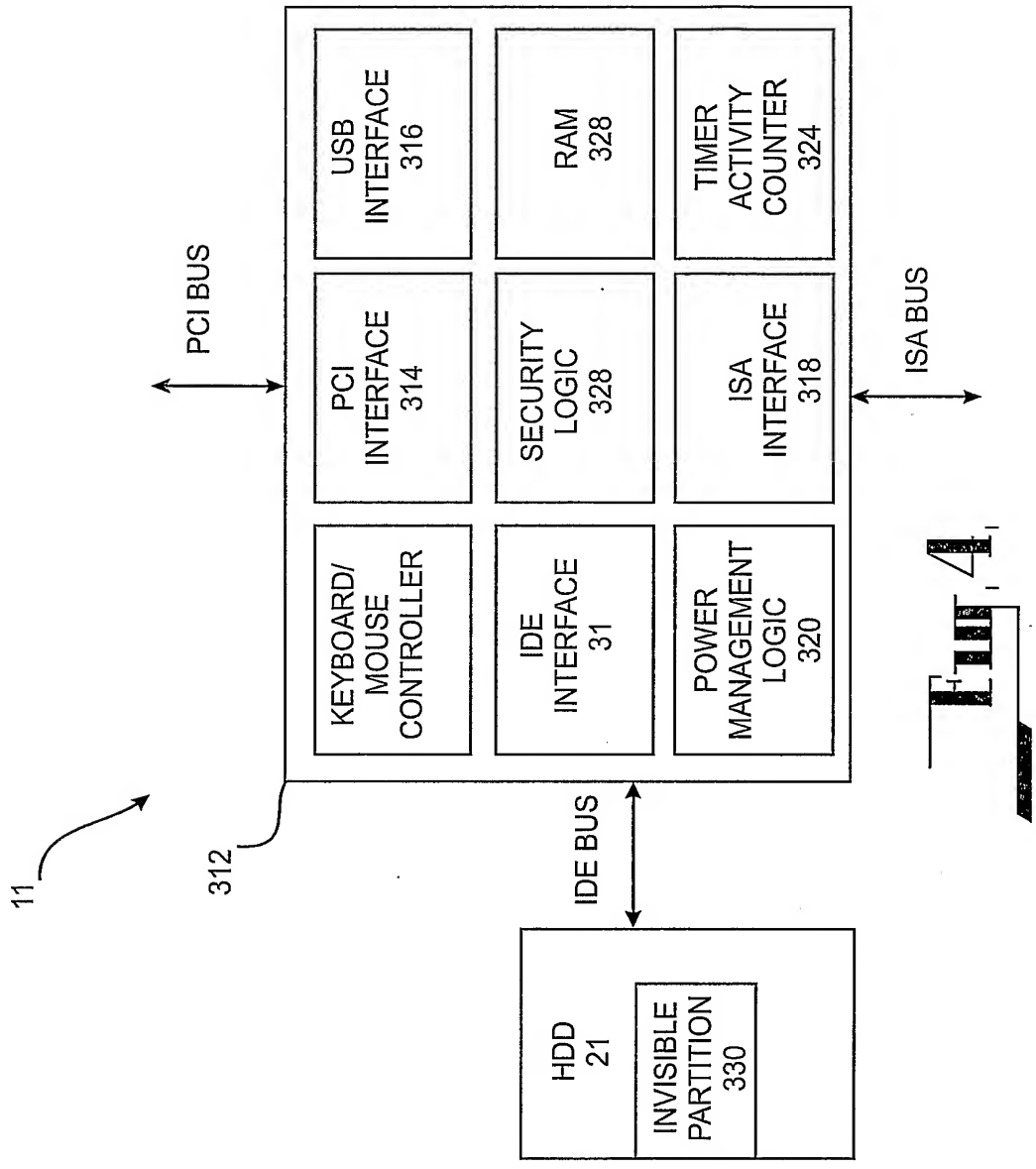

11
312
PCI BUS
ISA BUS
IDE BUS
KEYBOARD/ MOUSE CONTROLLER
IDE INTERFACE 31
POWER MANAGEMENT LOGIC 320
PCI INTERFACE 314
SECURITY LOGIC 328
ISA INTERFACE 318
USB INTERFACE 316
RAM 328
TIMER ACTIVITY COUNTER 324
HDD 21
INVISIBLE PARTITION 330

Fig. 4

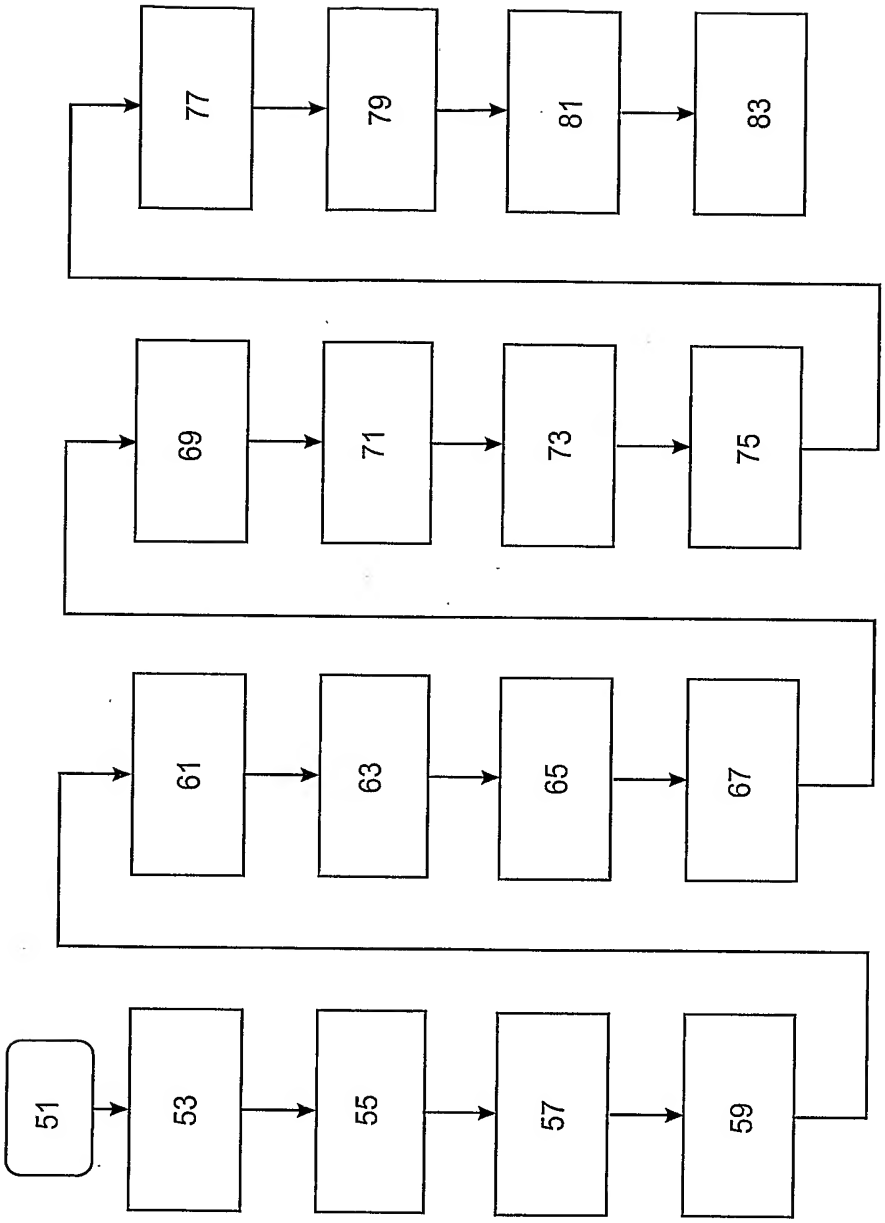


Fig. 5

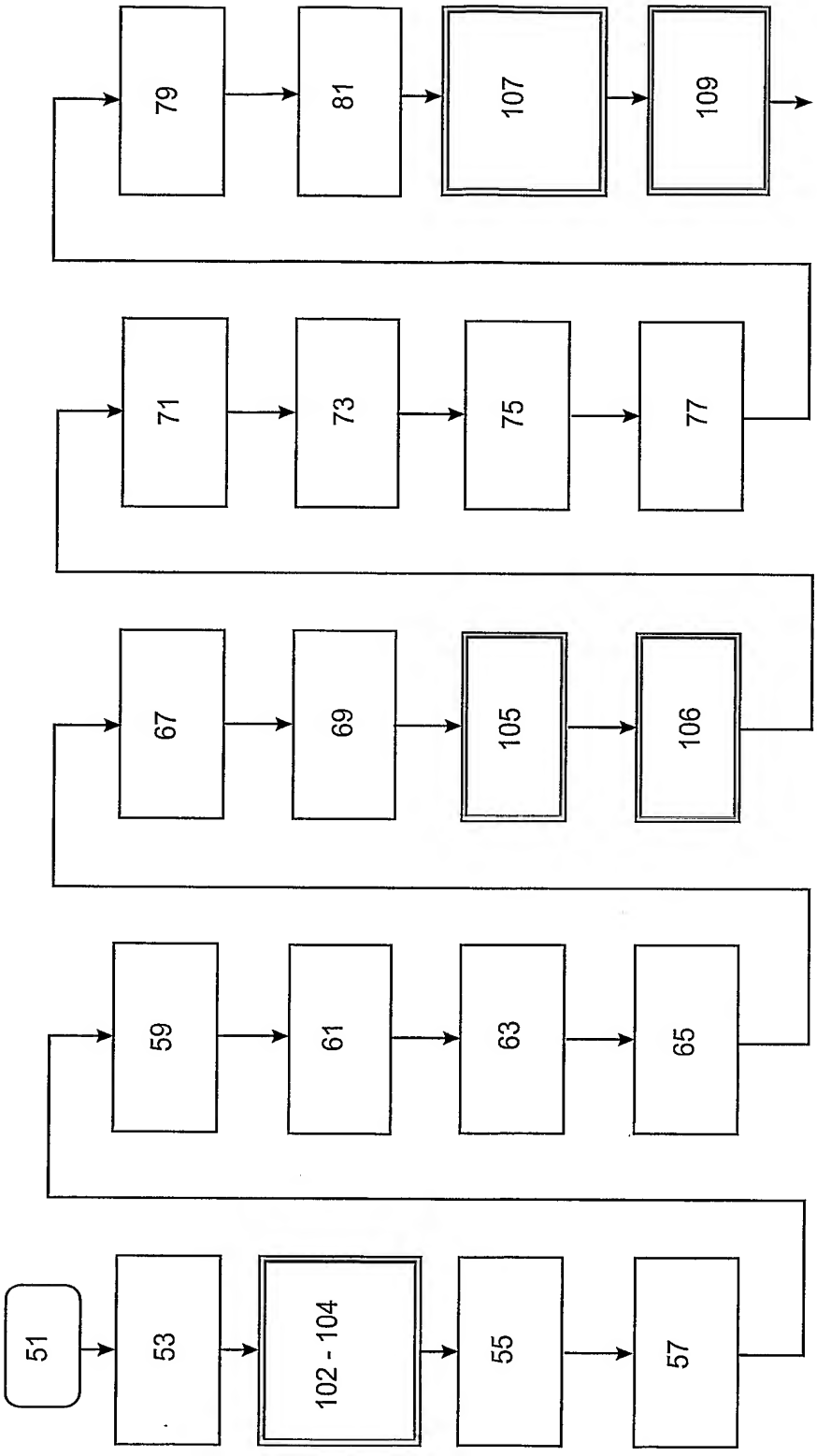

51
53
102 - 104
55
57
59
61
63
65
67
69
105
106
71
73
75
77
79
81
107
109

Fig. 6A

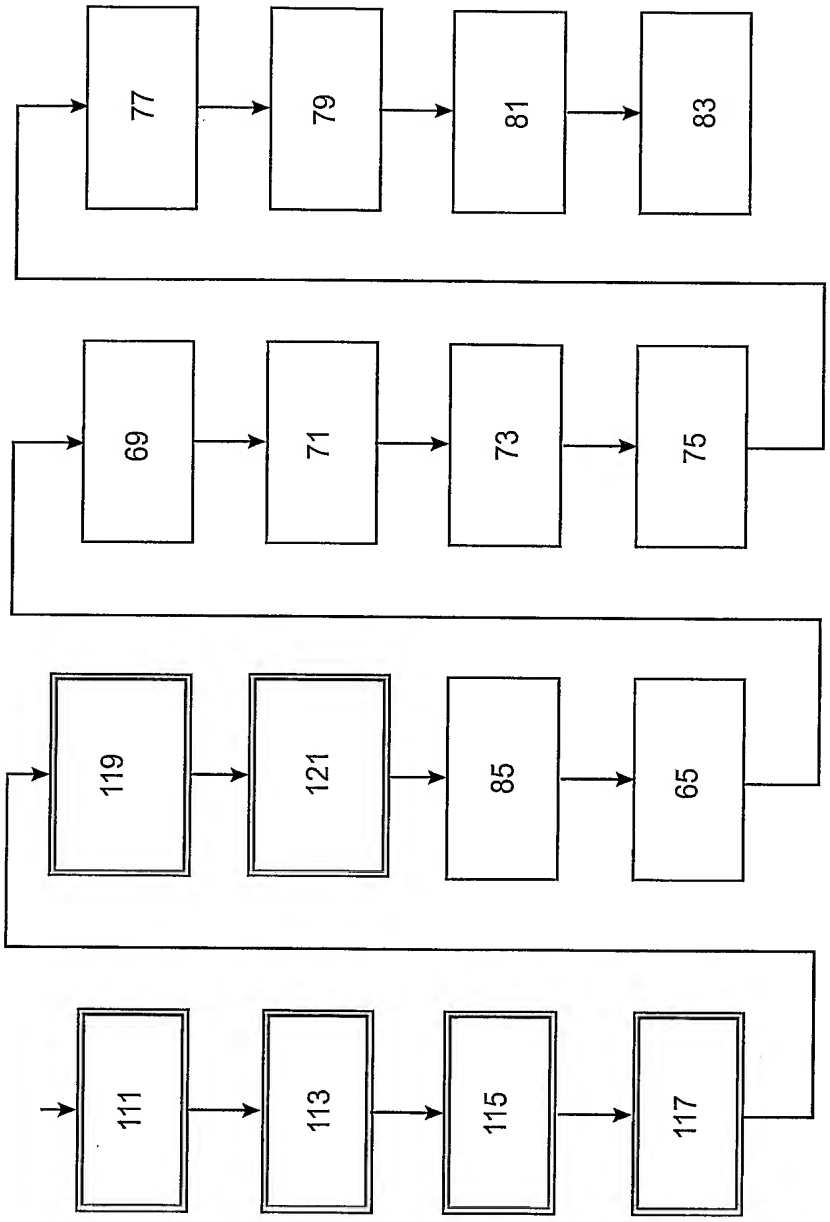


Fig 6B

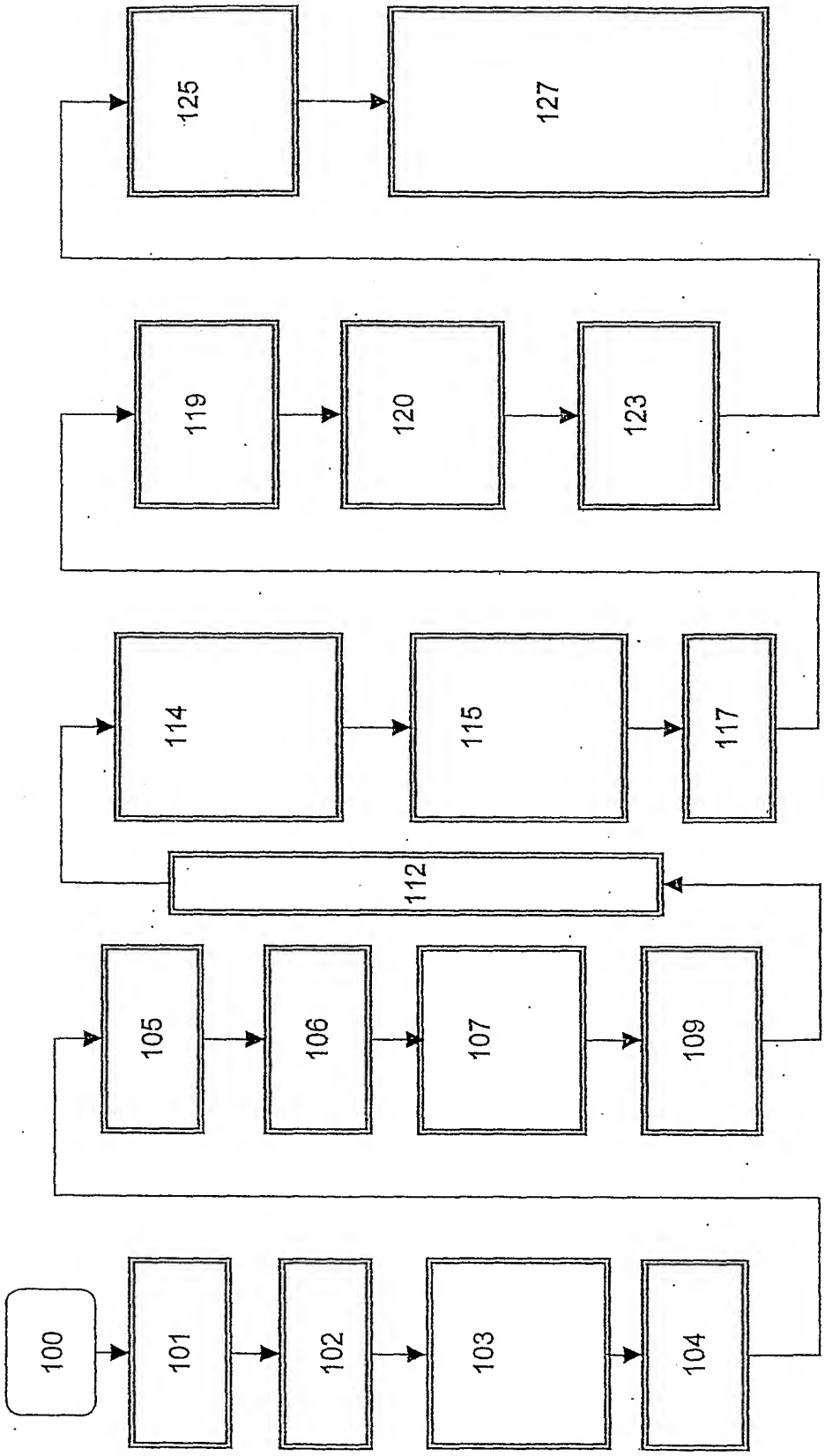

100
101
102
103
104
105
106
107
109
112
114
115
117
119
120
123
125
127

Figure 7

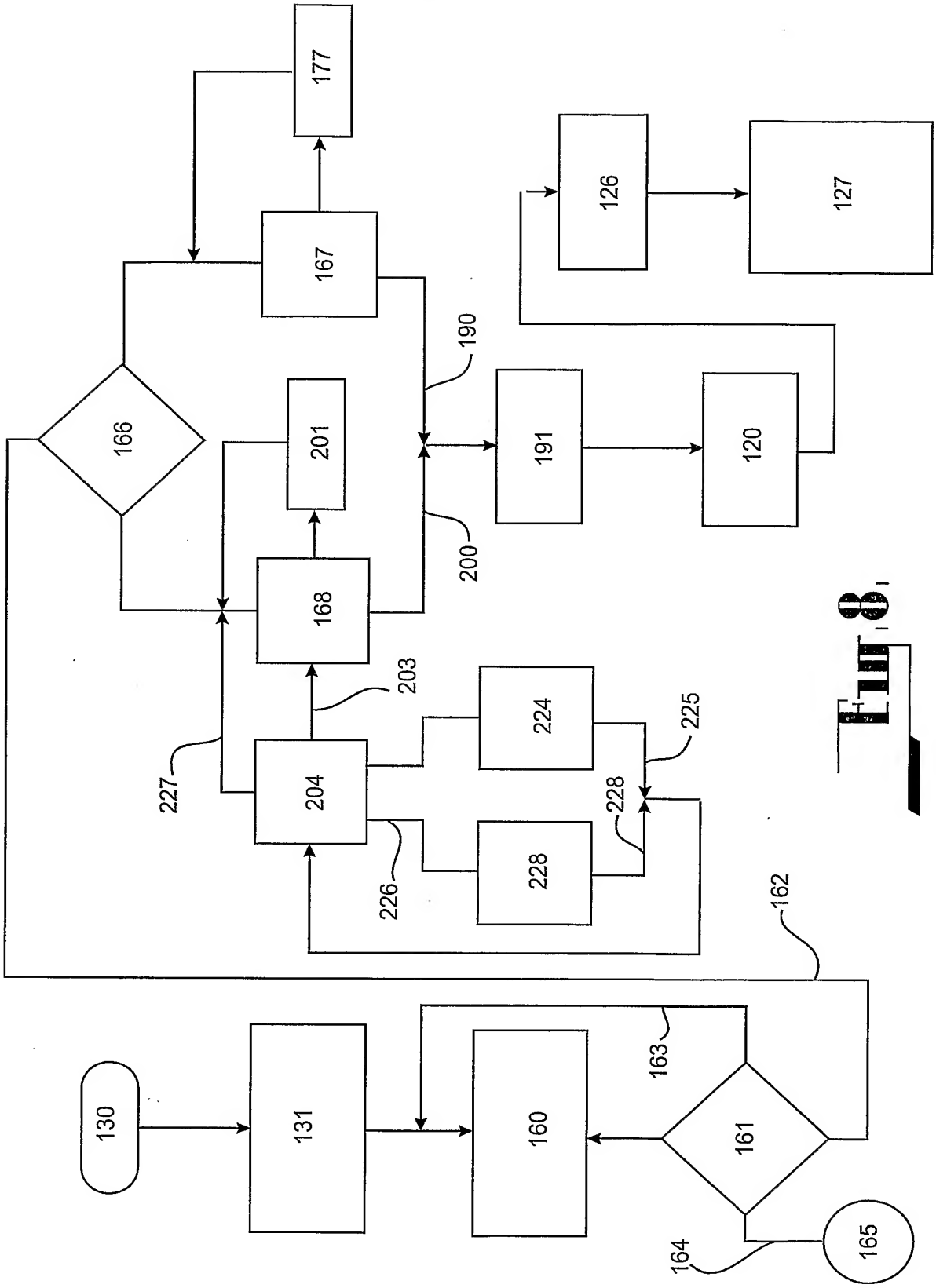

130
131
160
161
162
163
164
165
166
167
168
177
190
191
200
201
203
204
224
225
226
227
228
120
126
127

Fig 8

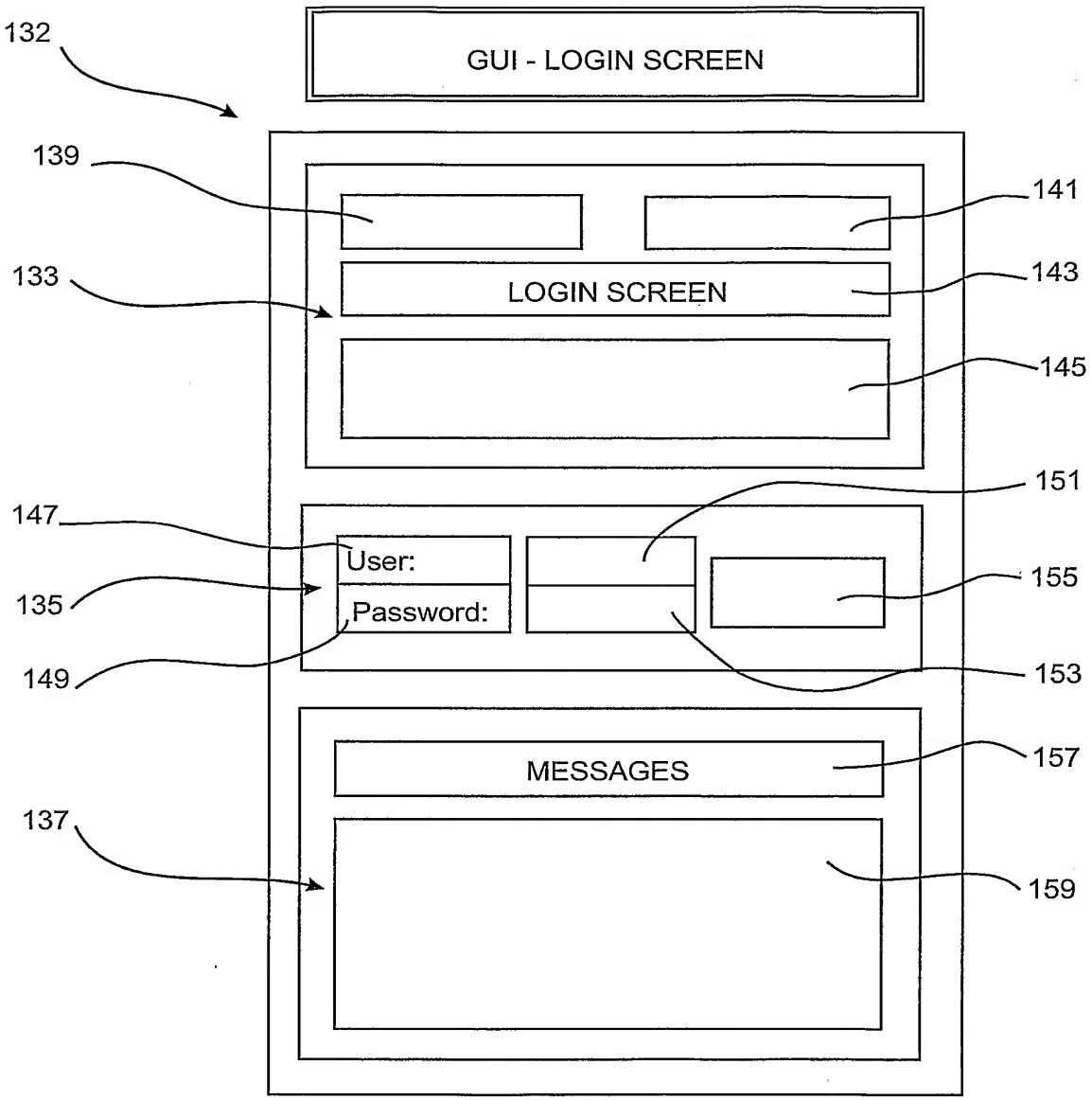

132
GUI - LOGIN SCREEN
139
141
133
LOGIN SCREEN
143
145
151
147
User:
135
Password:
155
149
153
157
MESSAGES
137
159

Fig. 9A

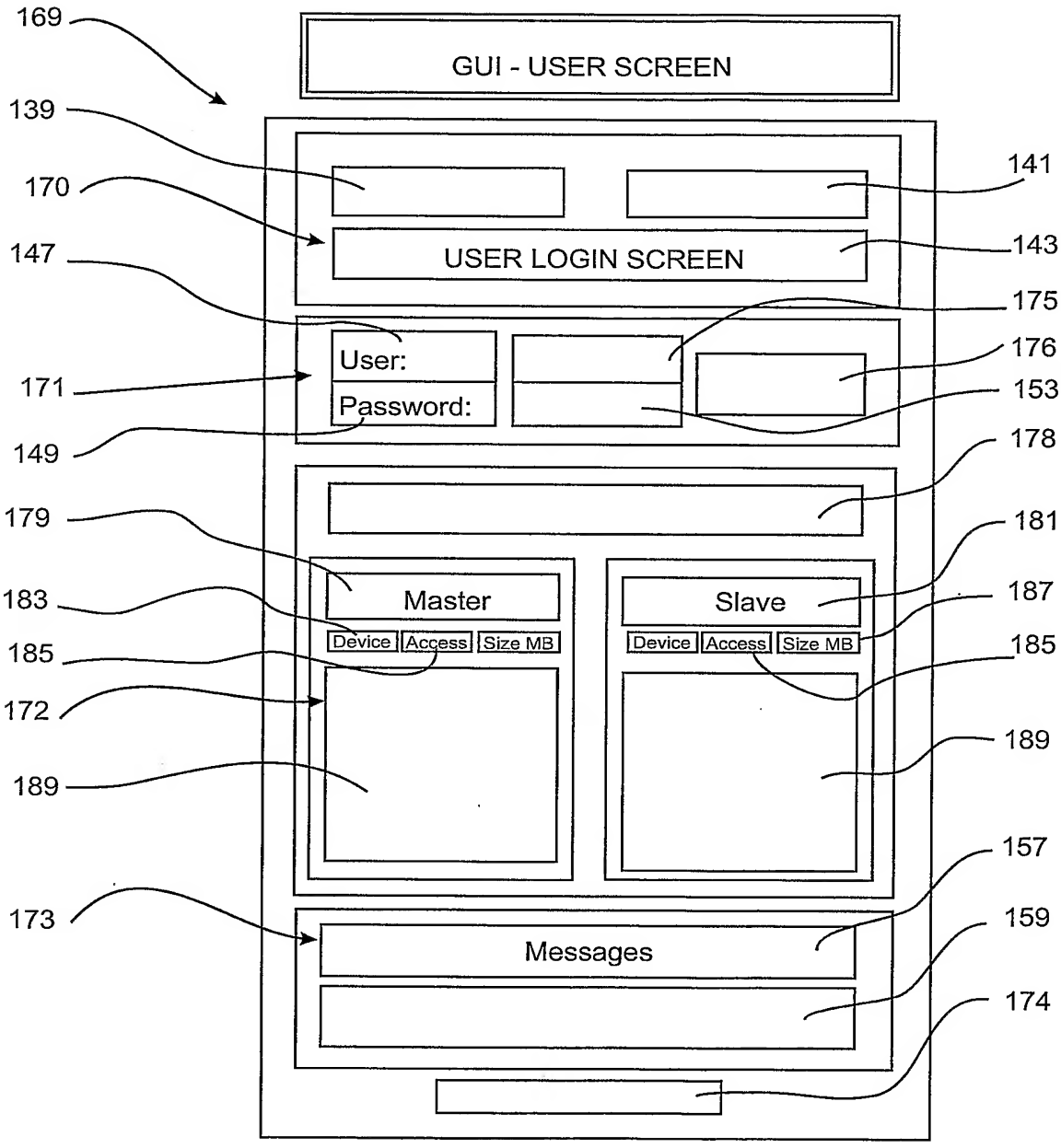

169
GUI - USER SCREEN
139
141
170
USER LOGIN SCREEN
143
147
175
User:
176
171
Password:
153
149
178
179
181
Master
Slave
183
187
Device
Access
Size MB
Device
Access
Size MB
185
185
172
189
189
157
173
Messages
159
174

Fig. 9B

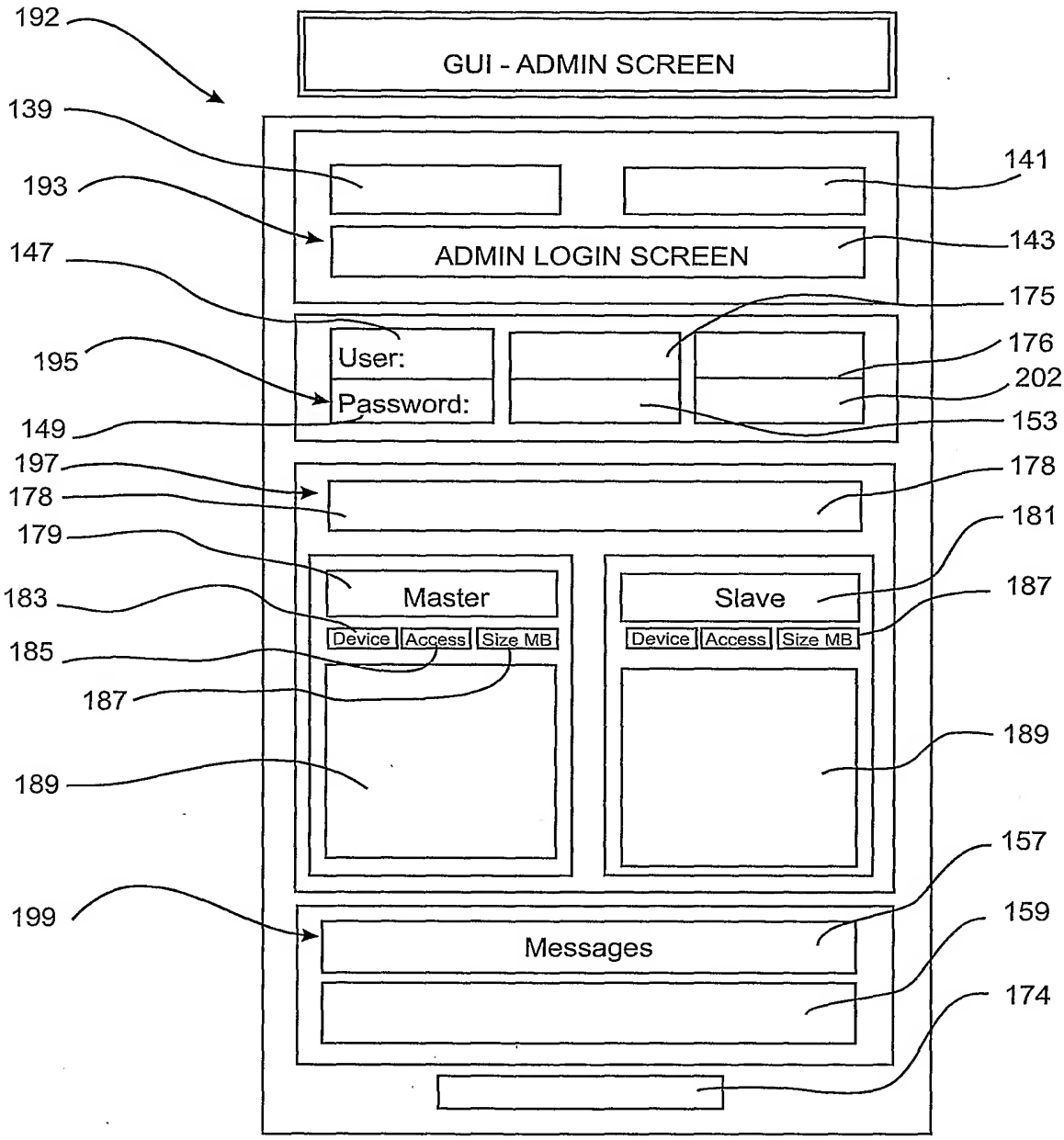

192
GUI - ADMIN SCREEN
139
141
193
ADMIN LOGIN SCREEN
143
147
175
User:
176
195
Password:
202
149
153
197
178
178
179
181
Master
Slave
183
187
Device
Access
Size MB
Device
Access
Size MB
185
187
189
189
157
199
159
Messages
174

Fig. 9C

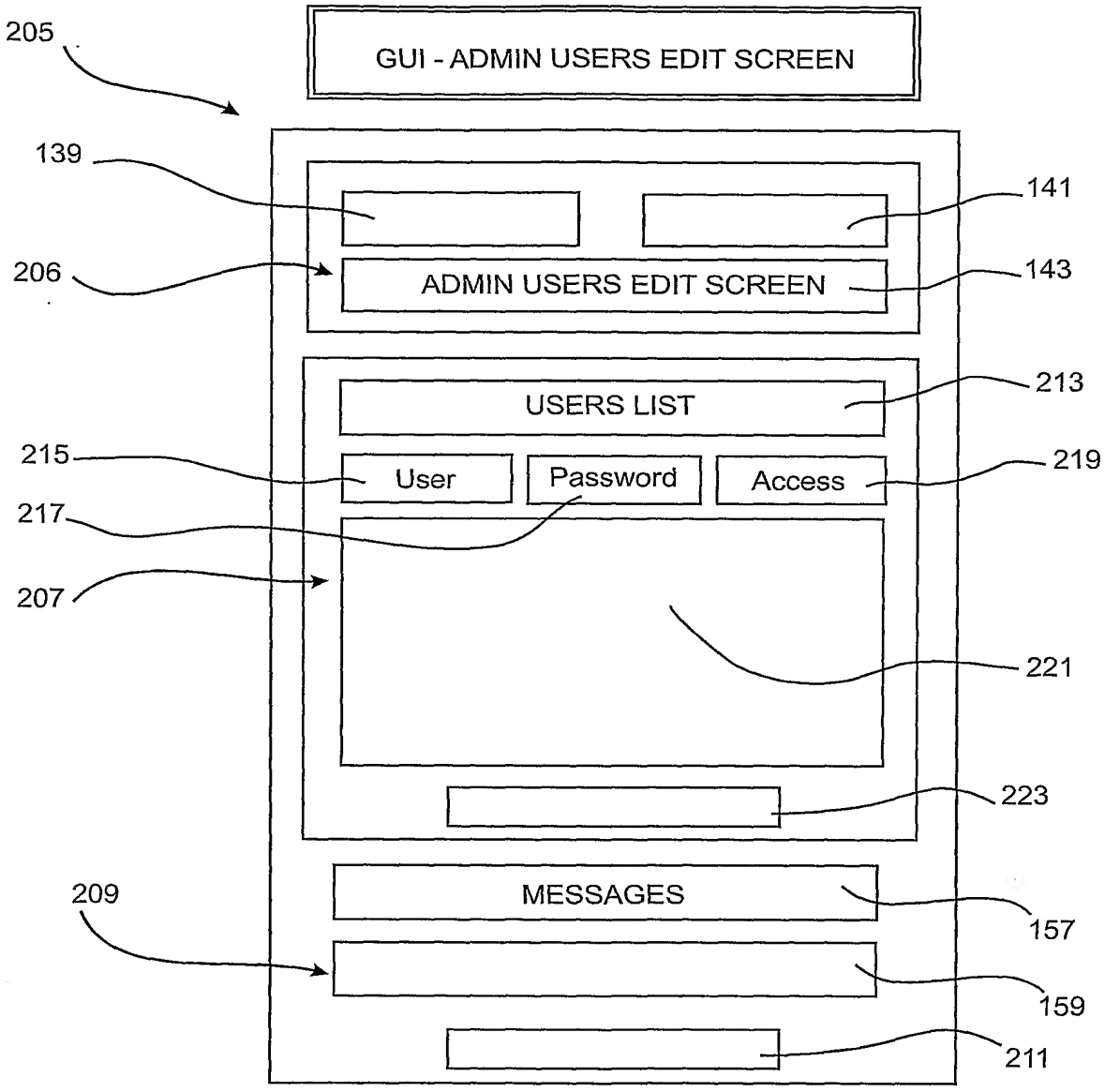

205
GUI - ADMIN USERS EDIT SCREEN
139
141
206
ADMIN USERS EDIT SCREEN
143
213
USERS LIST
215
User
Password
Access
219
217
207
221
223
209
MESSAGES
157
159
211

Fig. 9D

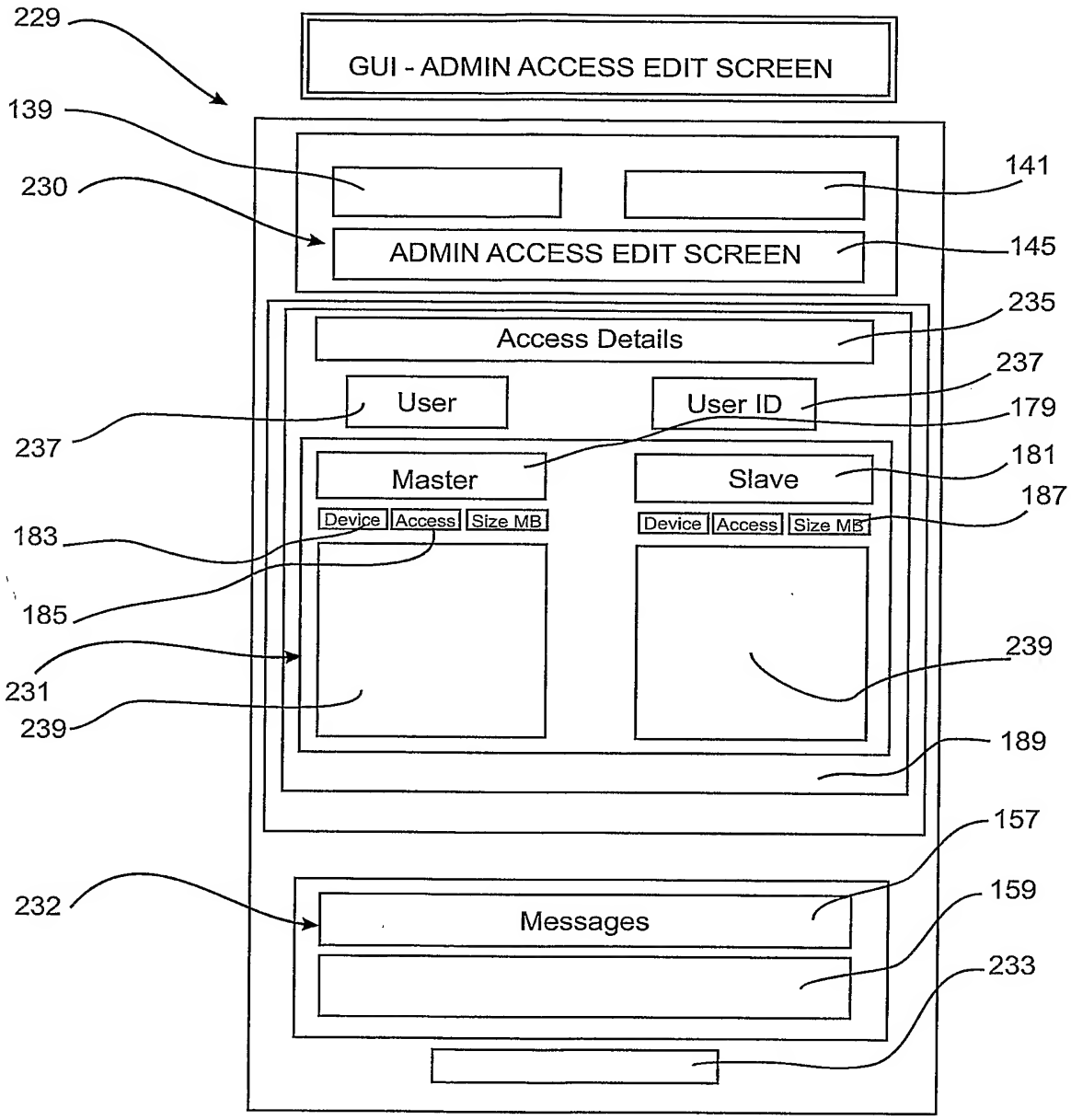

229
GUI - ADMIN ACCESS EDIT SCREEN
139
141
230
ADMIN ACCESS EDIT SCREEN
145
235
Access Details
237
User
User ID
179
237
181
Master
Slave
187
Device
Access
Size MB
Device
Access
Size MB
183
185
231
239
239
189
157
232
Messages
159
233

Fig. 9E.

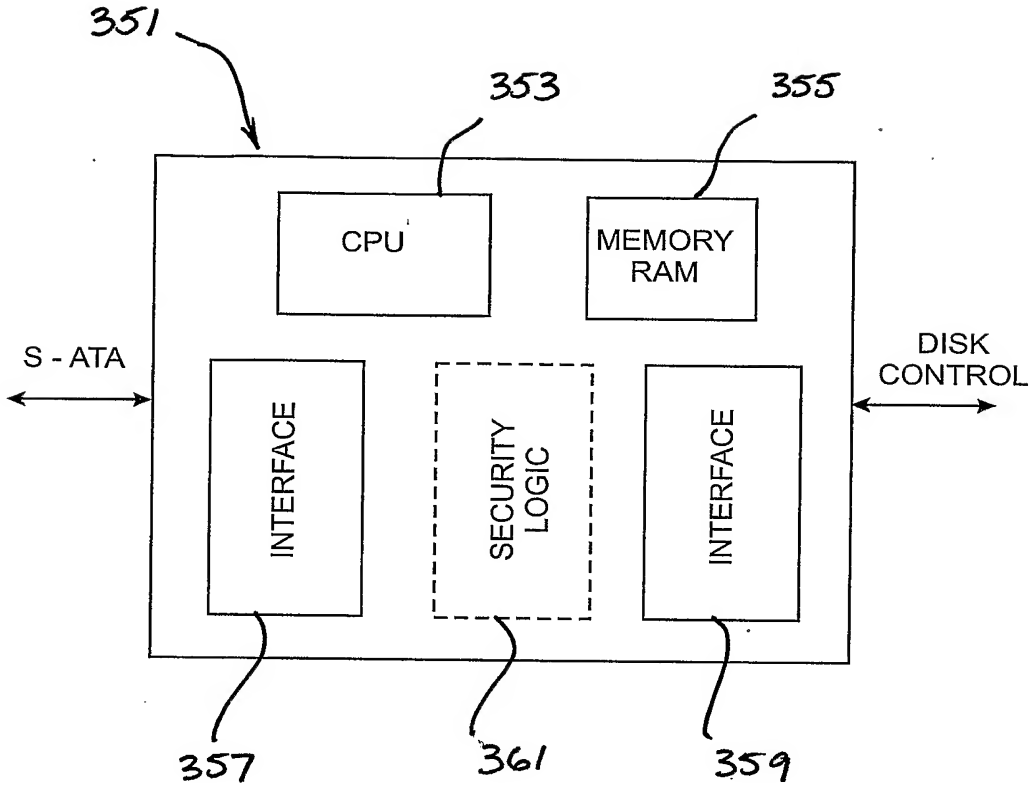

351
353
355
CPU
MEMORY
RAM
S - ATA
DISK
CONTROL
INTERFACE
SECURITY
LOGIC
INTERFACE
357
361
359

Fig. 10

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU2004/000210

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G06F 9/445, G06F 12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
DWPI,USPTO (bus, bridge, CPU, storage, security, boot, access, logic)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
	WO 2002/093335 A2 (ADVANCED MICRO DEVICES, INC.) 21 November 2002	
X	Abstract, claims, figures 1A, 4, 5A, 5B,6	1,2,12-14,27-31,33-35,42-63,65-69
Y	Whole document	1-72
	US 6199167 B1 (HEINRICH et al.) 6 March 2001	
X	Abstract, Claims	1,12,27,33,42,54,65
Y	Whole document	1-72
	WO 2003/003242 A1 (SECURE SYSTEMS LIMITED) 9 January 2003	
X	Whole document , especially claims	1,12,27,33,42,54,65
Y		1-72
	WO 1997/037305 A1 (INTEL CORPORATION) 9 October 1997	
A	Abstract, page 4 lines 13-18, page 5 lines 15-31, page 6 lines 1,2, claims	1-72

☐ Further documents are listed in the continuation of Box C ☒ See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 March 2004	30 MAR 2004
Name and mailing address of the ISA/AU	Authorized officer
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	**DALE SIVER** Telephone No : (02) 6283 2196

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU2004/000210

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
WO	02093335	US	2003028781	US	2003041248	WO	02093336
US	6199167	EP	0945777				
WO	03003242		NONE				
WO	9737305	CA	2219000	EP	0976025	US	5802069
		US	5887989	US	5903774	US	6009527
		WO	9718510	WO	9733228	WO	9737308

END OF ANNEX